NPS-CS-03-002

NAVAL POSTGRADUATE SCHOOL
Monterey, California

NAVSUP Hosting Requirements and Service Level Agreements

by

Leonard T. Gaines

06 January 2003

Approved for public release; distribution is unlimited.

Prepared for: Naval Postgraduate School
Monterey, CA 93943

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

RADM David R. Ellison, USN
Superintendent

Richard Elster
Provost

This report was prepared for Naval Postgraduate School as part of CDR Leonard T. Gaines' dissertation.

Reproduction of all or part of this report is authorized.

This report was prepared by:

Leonard T. Gaines
CDR, SC, USN

Reviewed by:

James B. Michael

James B. Michael
Dissertation Advisor, Department of Computer Science

Endorsed by:

Peter J Denning

Peter J. Denning
Chairman, Department of Computer Science

Released by:

D. W. Netzer
Associate Provost and
Dean of Research

REPORT DOCUMENTATION PAGE

Form approved

OMB No 0704-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
06 January 2003

3. REPORT TYPE AND DATES COVERED
Technical Report

4. TITLE AND SUBTITLE
NAVSUP Hosting Requirements and Service Level Agreements

5. FUNDING
None

6. AUTHOR(S)
Leonard T. Gaines

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Department of Computer Science
Naval Postgraduate School
833 Dyer Road, Code CS
Monterey, CA 93943-5118

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-CS-03-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Naval Supply Systems Command
5450 Carlisle Pike, P.O. Box 2050
Mechanicsburg, PA 17055

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words.)

This paper consists of a statement of work (SOW) and its related service level agreements (SLAs) for hosting services. The paper will be used as part of contract negotiations to outsource the hosting functions for NAVSUP owned applications. The SOW contains the hosting requirements that NAVSUP believes are necessary to support the application. NAVSUP will maintain control and responsibility of the application software, but all server and infrastructure hardware as well as system software support (operating system, monitoring software, utilities, and infrastructure software), is the responsibility of the service provider. The SOW details hosting requirements at three levels to allow program managers to select the levels and the corresponding services that best meet their needs.

A service level agreement (SLA) is an agreement between a provider of services and a customer that defines a level of performance. This agreement defines in measurable terms the service to be performed, the level of service that is acceptable, and the means to determine if the service is being provided at the agreed upon levels. SLAs define the quality of service, and how it is measured. There are fourteen SLAs defined that support the SOW.

This paper provides a starting point for negotiating host services. The intent of this paper is to give the program managers a document that listed hosting services that will provide a high level of support for their application. The SOW and SLA were designed to meet the needs of most applications, but each program manager will have the flexibility to select and modify the services and service levels required to support their specific applications.

14. SUBJECT TERMS
Service Level Agreements, Hosting Services, Outsourcing, Performance Based Contracting, Software Acquisition

15. NUMBER OF PAGES
120

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
UL

NAVSUP Hosting Requirements and Service Level Agreements

Leonard T. Gaines

Naval Postgraduate School

Abstract

This paper consists of a statement of work (SOW) and its related service level agreements (SLAs) for hosting services. The paper will be used as part of contract negotiations to outsource the hosting functions for NAVSUP owned applications. The SOW contains the hosting requirements that NAVSUP believes are necessary to support the application. NAVSUP will maintain control and responsibility of the application software, but all server and infrastructure hardware as well as system software support (operating system, monitoring software, utilities, and infrastructure software), is the responsibility of the service provider. The SOW details hosting requirements at three levels to allow program managers to select the levels and the corresponding services that best meet their needs.

A service level agreement (SLA) is an agreement between a provider of services and a customer that defines a level of performance. This agreement defines in measurable terms the service to be performed, the level of service that is acceptable, and the means to determine if the service is being provided at the agreed upon levels. SLAs define the quality of service, and how it is measured. There are fourteen SLAs defined that support the SOW.

This paper provides a starting point for negotiating host services. The intent of this paper is to give the program managers a document that listed hosting services that will provide a high level of support for their application. The SOW and SLA were designed to meet the needs of most applications, but each program manager will have the flexibility to select and modify the services and service levels required to support their specific applications.

NAVSUP Hosting Statement of Work

The scope of this document is to define the requirements for hosting Navy midrange application systems. Midrange systems are defined as those systems that fall between stand alone applications residing on a personal computer (PC), and those that reside on a mainframe computer. The scope assumes the Supplier maintains ownership of the servers, networking hardware, and associated systems software that is necessary to provide the hosting environment. It is not the responsibility of the Supplier to purchase or maintain application software unless otherwise negotiated between the Navy's Application Program Manager and the Supplier. The scope does not include hosting hardware that is owned by the Navy, which is referred to as co-location services. Although many of the requirements in this document apply to co-located hardware, co-location services are not part of this document and will be negotiated separately between the Navy and the Supplier. The government is contracting for a hosting service. The government does not intend to procure or maintain any of the hardware in the host environment. The Supplier is responsible for the hardware hosting the application. That allows the Supplier the flexibility to maximize efficiencies within their organization, resulting in a lower cost to the government.

This document is intended for production applications. It does not apply to test platforms, although this document can be easily modified to support that need. Test platforms will be negotiated under another contract vehicle with appropriate service level agreements (SLAs).

This document attempts to draw a clear line between application support, which is the responsibility of the program manager, and system software support (operating system, monitoring software, utilities, and infrastructure software), which is the responsibility of the Supplier. Any application support, other than monitoring, is outside the scope of this contract.

Essential Package System Support Areas

This statement of work (SOW) outlines three levels of support, the essential package, enhanced package and the premier package. The application's support requirements will dictate which package should be selected. If the enhanced package is selected, all of the services included in the essential package will also be included in the enhanced package. The premier service will also include services outlined in the enhanced package.

In addition to the services offered by each package, specified services can be added or deleted from the package. Adjusted services are outlined at the end of each package description.

The essential package is designed for stable, non-critical applications with minimal requirements for change, and predictable growth. As such, the services will reflect predictable capacity utilization, a consistent user base, and reliable application software.

Application Migration Service

Application Migration Services are the tasks necessary to transfer an application from one host environment to another. This seemingly simple task can be extremely complicated and difficult. A well-defined process needs to be implemented to ensure a successful migration. Migration services include information collection, platform and environment design, execution planning, testing, and ultimate deployment of the application.

Midrange Site Transition Services

Midrange site transition services must be available for moving Navy applications into the host environment. These services must include the use of a proven project management methodology and proven experience with transitioning similar applications.

Midrange Site Transition Services Requirements are:

- The Supplier will gather information on the application, develop a design plan for hosting the application, perform testing in accordance with the test plan, redesign if needed, prepare for ongoing production support services and deploy the application in a production environment.

The Supplier must obtain, assemble,, install, customize deploy, and tune network and server hardware, operating systems, and associated applications.

- The Supplier must coordinate with Navy Program Managers and technical staff to perform requirements determination and obtain a site survey of the application system being transitioned.
- The Supplier must develop a risk assessment plan. The Supplier must work with Navy Program Managers to identify and mitigate the risks associated with the transition of the application into the hosted environment.
- The Supplier must provide a project manager to oversee transition execution.
- The Supplier must provide a project plan with extensive detail, a work breakdown structure, and timelines to enable the execution to be managed and executed effectively within the Navy's operational constraints and business requirements.
- The Supplier must test the project plan execution in a test environment to validate the documented process and to confirm the defined production infrastructure supports the application and integrates into the host environment.
- The Supplier will work with the Navy application development team in developing a test plan to ensure the application performs as expected in the host environment. The Navy must approve the Supplier's test plan. The plan must outline the various tests to be performed, and establish thresholds for success. The Navy Program Manager must be responsible for functional testing, or for developing test scripts.
- The Supplier must ensure that the application's performance in the new production environment is equal to or greater than the performance the application demonstrated before the transition. Benchmark tests will be performed in both environments for comparison.
- The Supplier must test the application in a test environment before moving the application into production. The test of the application must follow the processes defined in the test plan. The test plan must ensure the testing environment emulates the application's production environment.
- The Supplier must provide project status or updates (at least weekly) of the plan from development through to implementation and post-migration.
- The Supplier must be able to execute the transition using a proven and repeatable set of processes that include multiple implementation options based on Navy requirements.
- The Supplier must provide a design solution for the hosted applications and be able to implement the solution.
- The Supplier must review implementation requests and the platform solution design with Navy Program Managers to verify the requirements, educate developers or

maintainers on the technology being employed, and ensure they understand the new architecture.

- The Supplier must interact with the identified network provider to help confirm that the platform configuration integrates the network requirements and connectivity is established to the Navy's LAN/BAN/WAN.
- The Supplier must ensure that applications that print to network printers have the necessary connectivity to the network and that the printer is properly set up on the server.
- The Supplier must verify that the appropriate hardware and system-level software products, for example, the operating system and non-application software, are obtained and ready to implement before the transition begins.
- The Supplier must work with the Navy technical staff to obtain, install and configure the application being transitioned.
- The Supplier must communicate migration support issues or implementation concerns through the site-specific communication process. The Supplier must provide progress reports to the Navy Program Manager as required.
- The Supplier must install and configure system-level software according to requirements defined in the platform solution design.
- The Supplier must work with the Navy Program Manager to define the backup and recovery needs for the application being transitioned.
- The Supplier must obtain signoff from the Navy Program Manager before going live with the application in the new environment.
- The Supplier must provide a final review of the implementation to determine whether the requirements have been met. Based on the final review, a production implementation live date is agreed to, at which point Transition Services end.
- The Supplier must incorporate the new application and associated hardware and software into all necessary documentation (e.g., hardware and software configuration documents, the backup plan, the disaster recovery plan, operation procedures, network diagram, etc…)
- The Supplier must complete a vulnerability assessment of the host environment (hardware, software and supporting infrastructure) that will be used to host the application. The information will be incorporated into the Supplier's System Security Authorization Agreement (SSAA) in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) program outlined in DoD Instruction 5200.40 to cover the host environment. This requirement is also included under the security section in more detail.
- The Supplier must provide the following documentation to the Navy Program Manager upon request: Project Plan, Risk Assessment Plan, Initial Configuration Audit, Design Solution, Results from initial audit of the application and the

requirements determination, Backup Plan, Disaster Recovery Plan, the Test Plan, and SSAA documentation.

Systems Management

Systems Management is the process of monitoring, evaluating, and reviewing the compute operation to determine whether operational requirements are met. The system management services included in the Essential Package are host system and network monitoring, performance monitoring, intrusion detection, automating compute operations, and system backup and recovery.

System and Network Monitoring

The System and Network Monitoring Services provide the operational support processes and procedures required for monitoring midrange compute environments for delivery of a stable, reliable functional environment.

System and Network Monitoring Services Requirements are:

- Monitoring of all network hardware (including firewall) must comply with NMCI, DoN, and DoD guidance and regulations.
- The Supplier should monitor application software status to determine if the application is responding.
- The Supplier must monitor all systems hardware and systems software that are used to support the application systems being hosted. Exclusions are listed below, however, monitoring for services on the list of excluded services must be available as a separate offering where indicated.

Exclusions are:

  - The Supplier should monitor application databases for space utilization and database performance and other specific database criteria such as dead locks (available under enhanced services).
  - The Supplier should monitor applications database to ensure the database is responding to requests (available under enhanced services).

- The Supplier must monitor all system consoles and logs. Console monitoring must be done using industry standard procedures and industry standard software. Some examples of industry standard monitoring software are: HP Openview, Cisco Works, CA-TNG, and NetScout. Console Monitoring Includes:
  - The Supplier must implement Event Detection Monitoring on the servers to detect any message sent to the system log and then cause an automated event to occur.
  - The Supplier must implement Network Monitoring on network assets within the host environment. Some of the monitoring functions include quality of service analysis, pinging an IP address or collecting data from an SNMP device on the network resulting in an automated event.
  - The Supplier must implement automated notification for console event alerts (e.g., e-mail, alarms, automatic trouble ticket generation).

- The Supplier must monitor network bandwidth for each application.
- The Supplier must monitor network bandwidth for the host environment network.
- The Supplier must monitor IP availability for each machine. Furthermore, selected sites on the Internet must be periodically (hourly) pinged to alert the staff to potential Internet problems.
- The Supplier must monitor web sites for hosted applications.
  Web Site Monitoring includes:
  - The Supplier must monitor polling of the Web site index (main) page.
  - The Supplier must implement automated notification for console event alerts if the site does not respond.
  - The Supplier must provide reports using a standard reporting tool on web site activities of the hosted applications (popularity documents, SLA compliance, report of the sites that access the user's Web server most often, etc).
  - The Supplier must provide monthly URL availability reports, if applicable, for the hosted application.
  - The Supplier must monitor URL availability to check the correct function of HTTP processes at timed intervals as specified by the Navy Program Manager.
  - The Supplier must monitor HTTP response times. A threshold will be set on a site-by-site basis; the party responsible for support is notified if the threshold is exceeded.
  - The Supplier must monitor HTTP Process Availability to ensure processes operating on the Web server do not have "out-of-bounds" conditions that may indicate an immediate or potential problem.

Performance Management

Performance Management processes include defining reasonable and measurable performance metrics, documenting and executing performance monitoring methods, maintaining contingency plans with corrective actions for exception performance, maintaining a support plan that incorporates the appropriate performance monitoring of documented requirements, reporting, implementing the monitoring activities, and measuring ongoing results.

Performance Management Services include the support processes to collect, monitor, and analyze system performance information, including, but not limited to:

- Processor(s) usage
- Input/output (I/O) throughput activity (e.g., operating system response time, disk access times, transfer times to disk, backplane speed, paging)
- Disk usage
- Memory usage

As needed, performance changes are implemented according to a change management process to modify the configuration and tune the system to optimize the effectiveness and efficiency of the midrange environment.

Performance Management Requirements are:

- The Supplier must maintain operating system parameters to manage performance and workload throughput. This includes tuning the system in the attempt to optimize the application's performance.
- The Supplier must monitor CPU, memory, I/O, and disk utilization against predetermined thresholds.
- The Supplier must monitor predetermined exception thresholds for Network bandwidth to assist in establishing monitoring alerts.
- The Supplier must provide monthly reports on CPU, Disk, and Memory utilization.
- The Supplier must provide monthly reports on network bandwidth and utilization.
- The Supplier must manage predefined exception thresholds for the operating system and major components to assist in establishing monitoring alerts.
- The Supplier must monitor real-time performance using system management tools to resolve system resource and performance problems.
- The Supplier must collect performance data dynamically to assist in problem determination.
- The Supplier must analyze historical performance data to isolate or identify potential performance issues.
- The Supplier must be able to recommend and implement workload allocation changes as they relate to applications use of server and network resources to assist the Navy Program Managers in resolving performance problems.
- Historical performance data will be retained for 1 year for trend analysis.

Capacity Management

Capacity Management Services include planning and monitoring system usage and capacity, both short-term and long-term, forecasting resource requirements, and analyzing and reporting resource trends. The Supplier's capacity processes should use metrics and reports that enable a clear understanding of overall performance and trends.

The Capacity Management Services Requirements are:

- The Supplier must perform resource usage analysis, including tracking, trending, and graphically illustrating resource usage by CPU, memory, I/O, storage, and tape consumption.
- The Supplier must provide reports, at least monthly, to the Navy Program Manager that show standard resource usage, trending and analysis. The Supplier must assist the Navy Program Manager in understanding the hosted applications current resource usage and future resource needs.

- The Supplier must use capacity planning to project the effects of new business and workload changes as needed. For example, the Supplier will perform capacity modeling when new business or application growth is anticipated, when substantial changes to existing business are anticipated, or when substantial configuration (hardware/software) changes are performed within the systems.
- The Supplier must take appropriate action to mitigate resource problems, including increasing the necessary resources. Additional resources needed to directly support the application as a result of an application change must be addressed at the Change Review Board. The Supplier will provide cost information associated with resource changes resulting from an approved application change. If the application change is approved, the program will be charged for the additional resources identified.

System Operations Automation

System Operations Automation Services include the use of Industry Standard automation software that provides for the automatic monitoring and remote reconfiguration of system environment resources or files to achieve operational efficiencies. Examples of Industry Standard automation tools are CA-TNG and HP OpenView.

System Operations Automation Services Requirements are:

- The Supplier must perform problem determination, day-to-day maintenance, and support for automation products and operational processes.
- The Supplier must be able to customize the automation requirements based on contracted services.
- The Supplier will continuously identify opportunities to remove manual interventions for ongoing support services.
- The Supplier will review automation software to ensure that they reflect the most recent policies and procedures.

Software Management

Software Configuration Management Services provide and maintain software for the operating environment, including operating system software and related system software. As part of these services the Supplier must perform the basic operating system software tuning that is required to maintain day-to-day operations.

Configuration Management

Configuration management involves the steps necessary to review and document changes to both the system software and the application, so that program manager and the Supplier are aware of maintenance or upgrades that may affect their application, or support processes. Accurate software configuration is essential when troubleshooting errors, performing software maintenance, and developing software (test beds should emulate production environment). Changes to the hardware or system software that impact the operations of the network, the servers, or the application must be reported to the Change Review Board (e.g. router configuration changes to close specific ports, or adding monitoring tools that impact server resources.).

The Change Review Board is chaired by the program manager for the application.. The Change Review Board consists of the program manager, design personnel, functional experts (if necessary), a representative from the Supplier's organization, government Information System Security Manager (ISSM) to address information assurance issues, and other personnel deemed necessary by the program manager or their chain of command. The intent of the Change Review Board is to approve any hardware or software configuration changes. The program manager and designers need to know if the Supplier's proposed changes will impact the application, or architecture. The Supplier must know if proposed application changes will affect resources, monitoring software, and network bandwidth. Additionally all approved changes are documented, improving communication channels, and ensuring only approved changes are implemented.

Configuration data will be held in a central repository that is web accessible. The repository will be populated using industry standard COTS packages, such as PVCS. The same configuration software should be used for all Navy applications.

Software Configuration Service requirements are:

- The Supplier must maintain documentation of server and network software configurations including OS release levels, configurations, patches, etc.
- The Supplier must, in coordination with Navy Program Managers, maintain documentation of application configurations including application software release levels, configurations, patches, etc.
- The Supplier must maintain documentation of all changes approved by the Change Review Board including date approved, change summary and date change applied.
- The Supplier must make all documentation available to the Navy upon request. The Navy program manager's staff will have web access to view configuration data held in the central repository.

System Product Integration and Problem Resolution

The Supplier must integrate the software components of the operating system and various third-party software products. System Product Integration and Problem Resolution provide the operational processes necessary to maintain a stable operation environment to meet the Navy's application specific operational requirements.

System Product Integration and Problem Resolution Services Requirements are:

- The Supplier must perform the planning, installation, testing, and upgrading of system-level software, such as operating system and other non-application software, or application software requiring super user access.
  - The Supplier must perform problem resolution including problem determination, interface, and escalation with third-party suppliers, if necessary, to correct system component problems.
  - The Supplier must participate in identifying system product problems including connectivity and associated network problems.

System Software Maintenance

System Software Maintenance Services provide ongoing maintenance and support for the software supporting the application. These services also provide preventive software maintenance services when required. System software also includes maintenance to the infrastructure (e.g., routers, firewalls).

System Software Maintenance Services Requirements are:

- The Supplier must assist the Navy technical support staff with installing applications software when root/Administrator access is needed and when loading the application software media into the hosted server.
- The Supplier must review product status and maintenance information for system patches to identify current version information and potential problems. All patches should be installed, unless there are mitigating circumstances. The program's Change Review Board must be notified of patches to be installed, and those patches that will not be installed.
- The Supplier must install preventive maintenance (e.g. software updates, software releases, and virus and anti-spam updates) to supported system software products to prevent known problems from impacting the operating environment.
- The Supplier must implement a permanent corrective action with appropriate monitoring procedures to ensure software faults are eliminated from the operating environment.
- The Supplier must communicate changes that require system down time to the Change Review Board. In the case of emergent changes that effect system availability the Supplier must notify the Navy Program Manager. If the change cannot wait for approval, the Supplier should notify the Navy Program Manager and the Change Review Board as soon as possible.
- The Supplier must ensure that the application has proper licenses for COTS products that are incorporated into the application. This includes accounting for usage-charged types of software agreements.
- The Supplier must review the Navy Program Manager's software service and licensing agreements and provide recommendations. Application consolidation may allow program manager's to reduce or eliminate some third party software requirements.

Software Refresh

Software refresh (system software, not application software) ensures that the software supporting the application does not become obsolescent. Technology is evolving at a rapid pace, and software must be updated to take advantage of new technology. Software Refresh Services Requirements are:

- The Supplier must plan for, install, and support new operating system, infrastructure and related system software. The plan must include the steps necessary for a successful migration of the application systems software.
- The Supplier must maintain a test system for systems software.

- The Supplier must work with the Navy Program Managers and Navy Technical Staff to research and resolve software compatibility issues allowing migration from the current suite of products to upgraded products and releases.

- The Supplier must have a documented software refresh plan. Some legacy applications currently in production have dependencies that do not allow for systems software upgrades and therefore should be exempt from this requirement. The application systems that should be exempt and their dependencies will be provided by the Navy Program Manager on an application-by-application basis. The refresh plan will have to be agreed upon with the Navy Program Manager and will have to take NMCI desktop systems into consideration.

- The Supplier must work with the Navy Program Managers to identify software changes that may impact applications. The Supplier will then work with the Program Manager to create a test plan, if necessary, to confirm that changes in software functionality do not adversely impact an application. The Supplier must address these changes with the Navy Program Managers at a meeting of the Change Review Board.

- The Supplier must design the necessary back-off processes to restore to the former operating environment if unforeseen problems occur.

Hardware Management

Hardware Configuration Management provides services for installing and maintaining the compute configurations to meet changing requirements for compute resources and maintains the configuration plan to meet application specific requirements.

Hardware Configuration Management

Configuration management involves the steps necessary to review and document changes to hardware used to support the application, so that program manager's staff is aware of changes that may affect their application.

- The Supplier must present hardware changes to the Change Review Board (CRB). Hardware changes resulting from hardware vendor requirements will still have to be briefed to the CRB.

- The Supplier must maintain documentation of hardware configurations, including equipment placement, network diagrams, cabling, connectivity details, application mapping, disk partition information, peripherals, etc.

- The Supplier must address new hardware installations or modification at a meeting of the Change Review Board.

Hardware Support and Maintenance

Hardware Support and Maintenance Services provide the support services necessary to ensure compute equipment is maintained, and operational. Hardware Support and Maintenance Requirements are:

- The Supplier must monitor midrange compute hardware, including processors, storage, and peripherals for malfunction.

- The Supplier must coordinate trouble-shooting, repair and, if necessary, escalation of hardware-related malfunctions with the hardware support vendor.
- The Supplier must manage hardware maintenance requirements based on the manufacturer's recommended schedule.
- The Supplier must coordinate and provide installation support hardware corrective maintenance requirements with hardware vendors.
- The Supplier must maintain documentation of all hardware changes approved by the Change Review Board including date approved, change summary and date change applied.
- The Supplier must make all hardware configuration documentation available to the Navy upon request.
- The Supplier must include a schedule for maintenance downtime. The downtime will abide by timeframes and duration specified in the service level agreements.
- The Supplier will have a documented preventative maintenance program for hardware support.

Hardware Refresh Services

The Supplier is responsible for replacing existing hardware components to include firewall, network, servers, etc. The Supplier will determine the hardware refresh rate, based upon their ability to meet requirements outlined in the service level agreements.

Hardware Refresh Services Requirements are:

- The Supplier must have a documented hardware refresh policy that includes migration strategies, timelines, accessibility, etc.
- The Supplier must coordinate planning, installation and testing, including shipping and receiving, of midrange compute hardware and environmental equipment.
- The Supplier must create a complete migration project plan and timeline and present the plan to the Change Review Board for approval.
- The Supplier must coordinate testing activities for the hosted applications with the effected Navy Program Managers.
- The Supplier must manage data migration and data movement processes, where possible, based on current hardware and software configuration to enable storage asset replacement.
- The Supplier must update documentation of hardware configurations, including equipment placement, cabling, and connectivity details as hardware configurations are refreshed.

Security Management

The Supplier must provide Security Management Services to protect the confidentiality, integrity, and availability of the Navy's information assets. The Services must adhere to all DoD, DoN policies and procedures (appendix (c) provides a list of relevant information assurance policies). Services include supporting data integrity protection software, user identification maintenance (authentication services), and password issuance. Server security must be monitored 24x7x365 unless an adjustment is made to the business hours of operational support coverage. Network security must be monitored 24x7x365 regardless of any adjustments. Physical security requirements for the hosting facility are defined as part of the Facilities requirements in the Enterprise Foundation section.

Security Management Services only address those areas that deal directly with the network, servers and associated hardware that support the Navy's application systems and do not address access to the application systems themselves. For instance, the Supplier must provide an identification and authentication mechanism for access to the application, but will not address or control identification and authentication mechanisms that allow access into the application itself.

The scope of these services includes the entire server farm from the firewall to the actual server. The firewall protecting the server farm is inside the scope of this SOW. The network from the end-user to the host environment firewall is not within scope for this SOW.

Security Management Services

- The Supplier must implement the appropriate INFOCON conditions when dictated by designated Navy personnel. The end users within NMCI must be able to maintain connectivity with the application during all INFOCON conditions.
- The Supplier must ensure that all personnel with access to government information have received the proper clearance from the government. Personnel without proper clearance will not be authorized access to any government data, nor will they be allowed to monitor any government applications.
- The Supplier must implement Root/Administrator Access Restriction/Verification – Access is restricted to a known set of Supplier support personnel.
- The Supplier must provide Vulnerability Scanning that identifies vulnerable configurations settings on network/system components, as well as identifying unauthorized ports/protocols and their associated applications. The scans must be periodically reviewed to provide a secure environment.
- The Supplier must run periodic (once a shift) scans against systems comparing current file permissions against an approved baseline.
- Security logs (server, firewall and network) will be reviewed once a shift at random hours. Although log entries can be sent to a central monitor it is necessary to physically review logs to discern patterns that may not be automatically detected.
- The Supplier must ensure that access to system-level files and services be restricted by use of operating system-level file permissions. The Supplier must maintain a database listing users, their access and permissions, their roles and security level.

- The Supplier must ensure that access through routers and firewalls adhere to the NMCI, DoD, and DoN Network requirements as they relate to protocols and specific IP address or ranges.
- The Supplier must ensure that security changes are processed, reviewed, tested and approved by Supplier and Navy Change Review Board before implementation.
- The Supplier will use base DoD and DoN configurations for server and network installations when they are available.
- The Supplier will configure each system platform based on a government supplied secure configuration guide. IAVA/B/TA will be implemented as required by DoN. Attachment (b) provides the listing of Secure Configuration Guides.
- DoD System Administrators will be properly trained and certified in accordance with the Office of the Secretary of Defense (DoD Memorandum dated 29 June 1998). This is a requirement for government agencies only.
- The Supplier is responsible for revoking all access rights and privileges of the Supplier's employees that were transferred, are retiring, or have been terminated. The Supplier must notify the Navy Program Manager that those individuals are no longer working on the project.
- The Supplier will provide a security point of contact or contacts to interface with the government on matters relating to information assurance issues.
- The Supplier will provide government access (customer, Naval audit) to the applicable information assurance documentation (logs, procedures) in accordance with the Government Information Security Reform Act (GISRA) with is part of section 811 of the Defense Authorization Act.
- The applicable System Administrator for each platform/system will maintain a repository of access request forms and user agreement forms for administrator accounts for their platform/system. The application administrator will maintain a repository of access request forms and user agreement forms for user accounts.
- The applicable platform/system systems administrator will ensure all non-public web sites implement identification and authentication mechanisms (e.g., user id/password, DoD PKI certificate, CAC card with hardware certificate), and are SSL enabled with a DoD PKI server certificate. The systems administrator will ensure the server certificate is renewed prior to expiration date.

Intrusion Detection Services

The Supplier must incorporate Intrusion Detection Services using an Intrusion Detection System (IDS) that is designed to monitor the network for known security threats.

Intrusion Detection Services Requirements are:

- The Supplier must implement an industry standard (NSA approved) IDS that enables real-time notification of potential security problems, such as denial-of-service attacks or other security breaches.

- The Supplier must implement an industry standard (NSA approved) IDS that monitors inbound network traffic for numerous attack signatures. In the event of an intrusion alert, the Supplier must be automatically notified and appropriate action must be taken based on the alert's nature.
- The Supplier must implement the most current versions of software that recognize activity patterns of known attack signatures.
- The Supplier must provide monthly reports of security incidents to the government.
- The Supplier must notify the affected government Program Managers if an intrusion is successful and provide an assessment of the damage.
- The Supplier must have sensors in place that monitor network traffic and search for known attack signatures.
- The Supplier must use agents that monitor the network and analyze audit logs and search for attack signatures and policy violations.
- The Supplier must have a console to remotely manage the sensors through authenticated and encrypted communications.
- The Supplier must use an automated incident response capability that may reconfigure firewall rule sets to repel an attack.
- The Supplier must use automated notification to administrators in the event of an attack.
- The Supplier must utilize authenticated and encrypted (128-bit) communications between sensors/agents and consoles.
- The Supplier must ensure that sensors/agents are hardened from attack. This is usually done by ensuring the integrity of the software through products that create an encrypted hash of the file.
- The Supplier must notify the affected government ISSM and program manager within 30 minutes if an incident causes service degradation/disruption or if a successful intrusion occurs. The Supplier will complete the Navy Incident Report (see appendix c) with assessment of the damage, and provide a copy to the ISSM in accordance with the timelines outlined in instruction OPNAVINST 2201.2.
- If an intrusion is successful, the Supplier will notify the appropriate government personnel and activities within the timeframes established in the SLA.

Vulnerability Assessment

The Supplier will have a developed perimeter vulnerability assessment methodology specifically designed to determine an organization's overall vulnerability to Internet-based attacks, along with identifying exposures and risks associated with any of the organization's firewalls, FTP servers, Web servers, DNS servers, and e-mail servers residing on their Internet perimeter.

This assessment will run remotely, probing the Internet/Intranet perimeter for all hosted applications in the same way a "hacker" would. The process will identify weaknesses in the hosted network and system configurations, thus providing the capability to immediately address and correct any identified deficiencies or shortcomings.

This vulnerability assessment is separate from the "red team" assessment, which is a government-funded assessment. Service Level Agreements will dictate the metrics used to determine compliance with regard to the "red team" assessment. The assessments discussed in this section will be undertaken by the Supplier to prepare for the government assessments.
Vulnerability scanning will assess system vulnerabilities from two perspectives: network vulnerabilities and host-based vulnerabilities.

 - Network vulnerabilities are those weaknesses in systems and network components that could be exploited by an attack originating outside the system, including IP spoofing, TCP/UDP port attacks, SYN floods, and other denial-of-service attacks.
 - Host (operating system) vulnerabilities are weaknesses in systems that could be exploited at the system itself, including poor authentication, easily guessed passwords, and poor access control lists. System vulnerability detection also investigates system vulnerabilities on primary service entities such as servers, routers, and firewalls.

- The results of all Vulnerability Assessments are classified in accordance with the appropriate classification guide. The Supplier must provide personnel with the appropriate security clearance to conduct and review the assessments and produce a corrective action plan based on the results of the Assessments.
- Port Scanning runs an in-depth port scan of the platform on the host environment's Internet perimeter to identify "high-risk" services found running on the hosts visible to the Internet. The Supplier will take action to mitigate the risks associated with those ports.
- Vulnerability Assessment Scanning uses a variety of automated and commercially available tools to remotely probe the specified networks for security vulnerabilities, known software bugs, configuration problems, and unnecessary services, uncovering security weaknesses.
- The Supplier should also provide a periodic review of systems and administrative security controls to make sure that they meet or exceed NMCI, DoD, and DoN standards. The review is required to make sure that all changes made to security control mechanisms can be traced to a duly authorized security change request.
- Server Vulnerability Assessment is a service designed to determine vulnerabilities, exposures, and risks associated with the Navy's specific server(s). This will include completing a System Security Authorization Agreement (SSAA) in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) program outlined in DoD Instruction 5200.40 to cover the host environment. The SSAA will be made available to the Navy Program Manager for incorporation into their systems' SSAA. The application specific information required by the SSAA is the program manager's responsibility. The application specific information will be shared with the Supplier to ensure that the Supplier is aware of possible security problems that may affect the host network, systems, or

other applications. If an application evaluation is necessary to complete the application's SSAA, that task will be negotiated separately.

- The Supplier must ensure that vulnerability scanning adheres to all DoD and DoN security policies and procedures as they pertain to Networks and Servers.
- The Supplier must run the vulnerability assessment directly on the Web and application server(s), scanning the configuration for known security weaknesses.
- Supplier personnel must review the results of the server scan and provide a summary of findings to the Navy.
- The Supplier must provide one annual vulnerability scan run on the Navy's server – occurs just before the site goes online (LIVE URL); all other scans must occur at a minimum of annually.
- Real time Terminal in-state Residency (TSR) antivirus software protection will be implemented on each system to protect against malicious code as a result of file uploads/downloads.
- For DoD owned co-located servers, the DoD antivirus protection software may be used (DoD has already paid for an enterprise license).
- The Supplier must implement and maintain industry standard anti-spam software on servers running SMTP or E-Mail gateways.
- Upon report of an incident affecting the government application, the Supplier will allow FIWC to perform an Online survey (OLS) on the applicable network where the incident occurred. The OLS is an external probe that attempts to recreate the incident, or test to ensure the vulnerability that was exploited is corrected.

Data Protection Software Services

The Supplier will use Data Protection Software Service to ensure the integrity of essential data files. Data integrity processes and procedures will be in accordance with DoD, DoN policies.

Data Protection Software Service Requirements are:

- The Supplier must install, maintain, and administer security system software that controls user access to information on a midrange server platform, such as access control lists.
- Files containing passwords must be protected at the same level of protection as the most sensitive asset it protects or as "sensitive but unclassified data", whichever security level is higher.
- The Supplier must have processes, procedures and tools to maintain essential operating system and related system software data integrity.

User Identification (ID) Maintenance and Password Issuance

These services ensure only authorized users have access to their requested files and unauthorized access is denied without hindering business practices.

User ID Maintenance and Password Issuance Services Requirements are:

- The Supplier must use unique user identification (IDs) and passwords to control access.
- Identification and authentication mechanisms stored in the system must be encrypted in accordance with FIPS standards.
- The Supplier must execute DoN and DoD policies regarding password expiration times and minimum password lengths.
- The Supplier must be able to support Secured Network Communications. (i.e. SSL, PKI).
- The Supplier must provide the processes, procedures, and a security administrator to maintain unique user identification and password control access into midrange environments, not specific DBMS or applications.
- The Supplier must implement a system where the user is responsible for maintaining and changing their password on a server in accordance with the security policy.
- The Supplier must process authorized requests to create, delete, or change a user ID from an authorized submitter.
- The Supplier must provide the avenue to receive and respond to user problems in the areas of sign-on difficulties, password resets, and Logon/Login/Sign-On assistance. Response times are outlined in the service level agreements.
- The Supplier must maintain control of all Administrator/root access to all network and server hardware including applicable disk storage devices such as EMC RAID arrays.

Customer Support Services

The Supplier must have Customer Support Services that provide request management through a Supplier liaison. The Supplier liaison must provide a communication focal point to facilitate all systems support and professional services. Client Service Management for the Essential Services also includes business hours operational support coverage, problem management, and change management processes.

Request Management

The Supplier must have Request Management Services that provide a communications liaison to facilitate rapid response to the Navy's requests. These services must include coordination to receive and process the Navy's requests for services. Examples include Platform Solution Design Services, Site Migration Services, Software Refresh Services, and Shared Services to accommodate ongoing Navy business needs or growth requirements. Requests may also address a temporary service requirement, a temporary service level requirement, or the implementation of a long-term requirement in which the Service Level Agreement must be revised.

Request Management Services Requirements are:

- The Supplier must have a process to receive and execute requests.

- The Supplier must provide oversight and coordination to understand request requirements to ensure deliverables and timeframes are met for the execution of the requests.
- The Supplier must mediate scheduling conflicts between program managers that have applications residing on the same server.
- The Supplier must provide regular communication of issues, concerns, and request schedules and attend application systems meetings when requested by the Navy Application Program Manager.

Continuous Hours Operational Support Coverage

The Supplier must be able to provide continuous hours of coverage by skilled staff to support all selected compute management packaged services. The Supplier must provide all systems management functions from the Supplier's monitoring location 24x7x365 and all other Supplier personnel required to provide the selected packaged solution services must be readily available 24x7 as necessary. If continuous support is not necessary, services can be adjusted based upon application requirements.

Continuous Hours of Operation Support requirements are:

- The Supplier will have skilled staff to support the midrange environment and all Enhanced Services.
- The Supplier must provide a monitoring location with on-site leveraged staff to monitor 24x7x365.

Change Management

The Supplier must have a Change Management process that controls changes to the midrange compute environment. The Supplier's Change Management process will allow for the proper planning, analyzing, testing, communicating, and scheduling of hardware, system software, and environmental changes. Any changes made to the application, server software and hardware, or the infrastructure must be briefed at the Navy Program Manager's Change Review Board (CRB).

Change Management Requirements are:

- The Supplier must participate in the program's CRB as they are scheduled.
- The Supplier must document and track scheduled changes and status. Configuration documentation is available upon request.
- The Supplier must manage dependency requirements for all change scheduling.
- The Supplier must assist Navy Program Managers in assessing the risk of proposed changes, including review of change complexity, dependencies, duration of the change, ease of recovery, potential impact, and feasibility of the proposed implementation date.
- The Supplier must evaluate application changes to ensure that there is adequate resources and capacity to support the application.
- The Supplier must research and test all proposed system software upgrades and patches.

- The Supplier must manage and brief the status of proposed changes according to established CRB processes.
- The Supplier must assist Navy Program Managers in coordinating required testing to enable the successful implementation of changes.
- The Supplier must have a process in place that addresses the severity of change requests. The Supplier and the Navy Program Manager will determine the criticality of the change to ensure it is addressed in a timely manner as defined in the SLA's.
- The Supplier and the Navy must establish a mediation process to address changes that affect the contract, service level agreements or resource requirements.
- The Supplier must coordinate with the CRB in scheduling maintenance downtime and testing.
- The Supplier should document any tuning actions. If OS files are modified, that action should be documented. Routine tuning does not need to be presented to the Change Review Board.

Problem Management

The Supplier must have a developed Problem Management process that details the actions to be taken in response to operational issues. This process should enable timely communication of the status and corrective actions. Problem resolution must be prioritized based on the severity of the problem. As part of the Problem Management process it may be necessary to bring the critical application back on-line before the root cause of a problem is determined. If a problem persists, then the Supplier must coordinate a time with the Navy Program Manager to determine the root cause of the problem while allowing the application to be off-line for a longer period of time. For non-critical applications more time can be taken to determine the root cause of a problem.

Problem Management Requirements are:

- The Supplier must maintain a Help Desk with a centralized phone number for reporting and resolving problems. The Supplier's Help Desk must interface with the NMCI Help Desk because the Navy has designated that trouble calls be reported to the NMCI Help Desk first.
- The Supplier must prepare and communicate with the Navy Program Manager impact statements documenting the cause of the problem, the efforts required to temporarily correct the problem, a root cause analysis, and any follow-up steps. In addition to notifying the Navy Program Manager of a problem, updated status of the problem resolution, and estimated completion times must be provided as well.
- The Supplier must escalate any problems exceeding a response threshold based on severity of the problem. Thresholds are outlined in the service level agreements (SLAs).
- The Supplier must assist the Navy technical support staff if problem resolution points to the Navy application instead of the operating system or infrastructure.
- The Supplier response times will be determined by the negotiated SLA's.

- The Supplier must provide a monthly report to the Navy Program Manager with the appropriate help desk statistics, trend analysis, and a brief summary of the problems experienced, the means in which they were resolved, and the time necessary to fix the problem.
- The Supplier must coordinate with the Navy Program Manager to determine if they need to test the application to evaluate corrective action. All configuration changes resulting from the problem resolution must be documented and relayed to the CRB.

Service Level Management

The Supplier must provide Service Level Management Services through a communications liaison. The liaison must provide the avenue to understand and address the Navy's issues and concerns as well as be aware of the Navy's future plans, which would impact midrange services. The liaison will be the Navy's contact for reports and SLA issues and will work with the Navy's Program Managers to develop strategic and tactical plans for the hosted systems.

Service Level Management Requirements are:

- The Supplier must provide oversight of Service Level requirements and monitor and escalate any issues as necessary to help meet required Service Level standards.
- The Supplier must provide regular communications (weekly) and participate in joint planning processes (if necessary) with the Navy Program Managers and application teams to integrate service level management issues with directions on tactical and strategic planning; and near-term and long-term initiatives.
- The Supplier must work with the Navy Program Managers to develop a yearly IT plan that addresses Navy Program Manager requirements and the needs of the systems being hosted. The plan should include the expected growth rate of the application's user base, storage requirements, software releases, resource needs, future application releases, etc.

Standard Service Level Management Reviews and Reporting

This service provides quarterly Service Level Management Reporting and Reviews. The Supplier must provide reporting with data to measure conformance to the service levels on a quarterly basis. Additionally, the Supplier must provide application specific weekly change reports and quarterly trends reporting for all change metrics.

Standard Service Level Management Reviews and Reporting Requirements are:

- The Supplier must provide standard quarterly reports that outline the Supplier's services against those delineated in the Service Level Agreements.
- The Supplier must conduct quarterly review meetings to discuss service level reporting information.
- The Supplier will provide at least one weekly report that describes change activity for the midrange systems to include description of change, system affected, date and time of change, duration of change, and status of change for approved changes.

- The Supplier will provide a quarterly report of change activity metrics that includes the number of changes, number of successful changes, missed change windows, and number of changes not meeting lead-time requirements.

Business Continuity

Business Continuity involves the planning and implementation of procedures that ensure critical business operations resume following a disaster and that they return to normal operations as soon as possible. Part of the process is determining which applications are critical and which are not, then deciding upon the time frames for recovery and site recovery necessary to meet the recovery needs. Site recovery options are discussed in the Recovery Site Requirements section of the Enterprise Foundation Services of this document. Business Continuity is also referred to as contingency planning, recovery planning, business resumption planning, or disaster recovery planning.

Documented Recovery Action Plan

The Supplier must maintain a plan for recovering the midrange operating system and related system software. The Supplier must work with the Navy Application Program Managers to define the appropriate software recovery plans. The plans can be tailored to the solution defining the backup schemas, critical components, and test plans based on the specific workload. The recovery plan provides the processes, and documentation covering tape backups, recovery, and disaster recovery.

Documented Recovery Action Plan Services Requirements are:

- The Supplier must maintain documented recovery procedures for restoring the operating system and related system if a disaster occurs.
- The Supplier must conduct an annual review of the midrange environment to determine whether the operating system data backup and off-site storage rotation schedules meet recoverability objectives.
- The Supplier must have documented hardware and software configuration data to ensure the system is recovered to the most current environment.

System Backup and Recovery

The Navy needs to have operational support and management processes that meet operating system and related application requirements for data availability, accessibility, and retention. This service allows all system software and related storage configuration to be recovered if an operational or hardware failure occurs. This service supplements the Business Continuity Services that allow recovery if a disaster occurs. All backup media and the information on the media relating to the application or application database is the property of the Navy.

System Backup and Recovery Requirements are:

- The Supplier must implement backup software that monitors the backups via log files and reports any files that were not successfully backed-up.
- The Supplier must adhere to the documented backup plan to ensure that a minimum of one backup copy is maintained for each critical file. The normal backup schedule is where backups are performed daily 6 times a week and a full backup is performed

on Saturday or Sunday. Additionally a full monthly and end of year backup are performed. Unless increased by the Navy Program Manger the minimum retention requirements for backups are:

- Daily incremental backups
- Weekly full backups must be stored for 2 months
- Monthly full backups must be stored for 12 months
- Annual full backups must be stored for 5 years.

- The Supplier must implement backup software that verifies backed-up files by reading what was written.
- The Supplier must implement backup software that is able to perform unattended automatic backups of all systems.
- The Supplier must test full system restoration of the systems, including hardware, software and processes annually at a minimum or as specified by the Navy Program Manager. Results and lessons learned must be provided to the Navy Program Manager.
- The Supplier must have a process in place to facilitate requests for recovery of application specific files. The restoration times for each hosted application will be addressed in the application's SLA.
- The Supplier must monitor, verify, and escalate issues as necessary for operating systems and related application software backups and authorized restores.
- The Supplier must manage operational support processes for performing operating system and related application software recoveries as required in resolving software and hardware problems.
- The Supplier must adjust data backup and restore plans as new components are added to the system or availability requirements change.
- The Supplier must maintain the tape library to ensure the availability of the media and storage location to include scratch and foreign tapes.
- The Supplier must provide and maintain media including media reliability evaluation and aging and replacement processes.
- The Supplier must dispose of old backup medium in accordance with DoD and DoN policies.
- The Supplier must store the on-site backup medium in a separate space as the systems that are being backed up to ensure the safety of the medium in case of a disaster.
- The Supplier must transfer magnetically stored media to a new medium every three years to prevent degradation.
- At the conclusion of the contract, or if the contract is terminated for cause, the Supplier must deliver all application specific backup media and corresponding documentation to the Navy Program Manager.

- The Supplier must monitor and manage the SAN or NAS network if used.
- The SAN or NAS network can only be used to backup military/government applications. No civilian applications can utilize the same network to perform backups. The entire SAN or NAS network and system will be protected at the same level as the highest security classification of the information that it is backing up.
- Each tape must be protected in accordance with the highest security classification of any information on the tape. For example, if a tape contains information that is sensitive, but unclassified (SBU), and the tape also contains information from another application that is unclassified, the tape must be treated as SBU. Any confidential information on a tape makes the entire tape confidential.

Off-Site Tape Services

The Supplier must provide the processes necessary to ensure a copy of the operating environment (operating system, system software and application software) is stored in a secure, off-site location.

Off-Site Tape Services Requirements are:

- The Supplier must prepare tapes for shipment to the off-site tape vault.
- The Supplier must provide off-site vault storage for backup and recovery media.
- The Supplier must provide transportation of backup and recovery media to and from the vault.
- The Supplier must provide a mechanism for specifying which tapes are to be returned from the vault.
- The Supplier must audit the off-site storage location at least annually.
- The Supplier must ensure that each tape is properly documented and labeled.
- The Supplier must ensure that at a minimum the full weekly backups are stored offsite.

Disaster Recovery Test Service

The Supplier must be able to provide full testing for the documented recovery action plan. Testing verifies that the Disaster Recovery Plan meets the Navy's Application Program Manager's requirements. It also can be used to evaluate how well the recovery plan integrates with the Supplier's other service providers to provide timely recovery from a disaster. At the Navy's discretion, network personnel, the application team, and some set of the user base can be involved to test the recovered environment along with the Supplier's staff. After each test is complete, the Supplier must identify any deficiencies encountered and enhance the plan if required to meet the Application Program Manager's recovery objectives.

Disaster Recovery Test Service Requirements are:

- The Supplier must conduct annual recovery testing based on the recovery option chosen by the Navy's Program Manager for the specific application.

- The Supplier must be able to restore the operating environment from the data backups.
- The Supplier must verify and test operating environment functionality.
- The Supplier must coordinate with the application team and user base for testing time, as required.
- The Supplier must provide annual drill reports to include recommendations on procedural changes that can make data restoration time frames more cost-effective while meeting realistic recovery requirements.

Recovery Site Requirements

Recovery sites are necessary to meet the Navy's business continuity needs. The Supplier must offer three levels of recovery facilities – shell-site, warm-site, and hot-site. These options are linked to the Business Continuity Services described in the Essential, Enhanced, and Premier Packages. The shell-site option is mainly targeted for the Essential Package, which provides only off-site tape storage. The warm-site option most closely matches the Enhanced Package and the hot-site option aligns with the high availability services provided in the Premier Package.

This section is an extension of the Business Continuity Service requirements and is not meant as a replacement for any other requirements in this document. All other requirements for the hosted applications are implied in this section.

Hosted application systems will be designated as requiring one of three levels of recovery facilities. These are defined as shell-site, warm-site, and hot-site recovery sites. The Supplier must be able to provide each of these facilities. The Supplier must also be able to accommodate changes to an application system's recovery facility needs.

To reiterate the requirement is that the Supplier be able to provide these sites (through contracts, existing partnership arrangements, etc…), not that the Supplier has to actually has to own, staff, or manage these sites on a full time basis. Service level agreements will determine if a hot site is needed, and whether it will have to be staffed for contingency purposes.

Shell-Site Recovery Facility requirements:

- Must meet all the General Facility requirements excluding the Structural Requirements.
- No hardware is available to support the applications that are running.
- The facility used must not be in the same physical location as the production facility.
- Shell-Site recovery testing for critical applications must be done at least annually.
- A third party may provide the facility and hardware.
- Documented procedures for redirecting applications to the Shell-Site Recovery Facility must be developed and maintained by the Supplier.

Warm-Site Recovery Facility requirements:

- Must meet all the General Facility requirements.

- The facility used must not be in the same physical location as the production facility.
- A third party may provide the facility and hardware.
- For designated applications and systems the hardware equivalent to the production environment is available in the warm-site facility.
- Warm-Site recovery testing for critical applications must be done at least annually.
- Documented procedures for redirecting applications to the Warm-Site Recovery Facility must be developed and maintained by the Supplier.

Hot-Site Recovery Facility requirements:

- Must meet all the General Facility requirements.
- The facility used must not be in the same physical location as the production facility.
- The facility and hardware must be maintained in a standby operating environment or as part of a high-availability server implementation located in two physical locations.
- Hot-Site recovery testing must be done at least annually.
- Documented procedures for redirecting applications to the Hot-Site Recovery Facility must be developed and maintained by the Supplier.

Facilities - General Requirements

Facilities are defined in this section as the physical locations of the hardware. The services addressed in this section include but are not limited to electrical power, HVAC controls, structural characteristics of the areas where the hardware is located and security as it concerns the physical access to the areas where the hardware is located.
All Facilities must comply with DoN and DoD requirements.

Electrical Power

- The facility must have a clean energy source. Power fluctuations must not affect the equipment.
- In data centers, emergency power-off switches that shut off all power supplies must be installed and be readily accessible with posted notices showing their location. The Supplier must monitor the emergency power-off switches continuously.
- Backup electrical facilities (e.g., generators) are needed to ensure long term uninterrupted power. The facility shouldmust have n + 1 generators.
- Backup electrical facilities must be tested annually at a minimum.
- Each server must have access to a secondary power source.
- In the event of a power failure, Uninterruptible Power Supply (UPS) systems must be configured and tested to ensure safe operations of critical hardware for a minimum of 30 minutes and to carry the load until automatic switching to the backup power supply takes place.

HVAC and Climate Controls

- Facilities must be climate controlled and have environmental conditions conducive to multiple computer systems.

- The air conditioning unit must be included in the fire suppression system, so in case of a fire the A/C shuts off.
- Sensors and alarms must be installed in data centers to monitor the environment surrounding the equipment to ensure that climate controls remain within the levels specified by equipment design.
- The Supplier must monitor environmental controls and take actions based on detected problems or issues.
- Reports of the climate control systems must be generated monthly at a minimum.
- The computer room should have positive air pressure.

Fire Suppression

- The data center must have its own alarm systems.
- Fire Suppression must be a pre-action / dry pipe sprinkle system and a gaseous system such as the replacement agent to Halon 1301, called FM-200. These systems must meet the National Fire Protect Act 75 as well as comply with most NAVFAC requirements to ensure the overall system adheres to commercially acceptable standards.
- The facility must ensure that it has working smoke and heat detectors.
- Computer supplies (for example paper) must be stored in a separate location away from the computer equipment to minimize risk of fire damage.

Structural

- Drop ceilings must include smoke, heat and water sensors.
- The facility must have a raised floor to support connections and airflow.
- The facility must have a loading ramp or easy access for loading equipment.
- Raised floor loading capacities must be a minimum of 150 lbs. / sq. ft.
- Raised floor must support a minimum-rolling load of 600 lbs (272 kg.) over the entire floor.
- The minimum floor loading capacities for the mechanical, electrical and battery room must be 400 lbs / sq. ft.
- Exterior walls should be able to withstand wind loads of 115 mph (185 kph). This is equivalent to a 'class 3' hurricane.
- Exterior envelope wall and roof deck composites should include a vapor barrier.
- No windows or curtain walls will abut the area where servers are located.
- Servers must not be housed in areas subject to flooding or water infiltration through walls, floors or ceiling.
- Walls separating critical mechanical and electrical equipment rooms must extend from the floor slab to the bottom of the roof or floor deck above and must be constructed with a minimum of a 2-hour fire rated assembly.

- Walls surrounding mission critical equipment in the data center areas must be constructed with a minimum of a 1-hour fire rated assembly.
- Walls surrounding magnetic tape and other media storage must extend from the floor slab to the bottom of the roof or floor deck above.
- Walls surrounding magnetic tape and other media storage must be constructed with a minimum of a 2-hour fire rated assembly.
- Blueprints must be available with markings for the following:
  - Power Supply
  - Fire Suppression
  - Access Points
  - Point of Presence to outside networks (PoP)
- The Supplier must comply with all Uniform Federal Accessibility Standards (UFAS) and must incorporate the American Disabilities Act (ADA) in its structural designs.

WAN/BAN/LAN Connectivity

- The Supplier must provide the service to connect geographically separated Navy and Marine Corps users/devices/printers. The Supplier must provide connection to external networks, for example:
  - Non-Secure IP Router Network (NIPRNET)
  - Secure IP Router Network (SIPRNET)
  - FTS-2001
  - Defense Research Engineering Network (DREN)
  - Defense Switched Network (DSN)
  - Public Switched Telephone Network (PSTN)
  - NMCI provided wide area transport services (commercial/DISA)
  - The Internet
- The Supplier must provide service to interconnect geographically co-located Navy and Marine Corps LANs and BAN attached devices.
- The data center's network must conform to DoD and DoN Internet and Intranet security policies.

Facility Physical Security

- Data center personnel are required to have picture identification badges.
- The Supplier must adhere to the personnel guidelines outlined in section 1.1.4 Contractor Specific Internal Information Guidelines of the N/MCI Contract N00024-00-D-6000 Attachment 4 Security Requirements document. Section 1.1.4 of the N/MCI Contract N00024-00-D-6000 can be found in Appendix A.

- Visitors must sign in and be escorted into and out of the facility to provide an audit log.
- A log of physical access to controlled areas must be kept.
- A list of individuals authorized to grant physical access to controlled areas must be maintained.
- A list of individuals granted physical access to controlled areas must be maintained.
- Access to secure areas must be protected by an electronic access control system.
- Access to data center equipment must be physically restricted to authorized personnel by locating the equipment in a closed area.
- The facility must have surveillance covering the entire server area 24x7x365.
- Detection devices or true floor to ceiling data center perimeter walls must be installed to prevent unauthorized access attempts.
- Physical security must implement multiple access control points with access controls to restrict access to authorized parties only (i.e. Tape Librarians should only have access to the tape library.)
- Attempts to gain unauthorized access to secured areas must be reported on a monthly basis.

Shared Services

Shared services are described as the use of shared servers and disk arrays that are utilized by multiple application systems. The Supplier must be able to use a strategy of leveraging its infrastructure to support the Navy's current and future business needs. Shared services should be used to help the Navy reduce its overall operations costs by making efficient use of available resources. Shared services should be available on a case-by-case basis determined by the supported applications requirements.

The application requirements are defined in the review of the application that is performed as part of the Midrange Site Transition Services for the application. As part of the review the Supplier and the Navy Program Manager will determine if shared services are appropriate for the application and if the use of shared services will enhance the performance, price and availability of the application in the hosted environment.

Shared Services – Disk

Shared Disk options include the use of current technology providing state-of-the-art speed of access to midrange disk components. The advantages of using Shared Disks are the availability of capacity on demand, application availability and economies of scale for large applications and databases.

Shared Services – Platform

Shared Platform Services are the use of state-of-the-art midrange servers that are able to support multiple application environments with the ability to reconfigure and reallocate server resources on the fly. These platforms may be implemented by the Supplier as a means of providing on-demand processing capacity and flexibility for the hosted application systems. Shared platform usage should be based on specific Navy application systems resource requirements as defined in the application requirements, selected SLA's and audit results.

Essential Services – Optional Service Upgrades

The Supplier must provide for service upgrades described in this section. The upgrades can be selected at an additional charge to expand the range of services provided in the Essential Package based on application-specific requirements.

Upgrade – No Upgrades defined for the Essential Services

Essential Services –Optional Service Adjustments

The Supplier must be able to adjust the service offerings for the Essential Services. These service adjustments can be selected to reduce the range of services provided in the Essential Services Package based on application-specific requirements.

Adjustment – No Documented Recovery Action Plan

This adjustment removes the Documented Recovery Action Plan Services from the Essential Services Package.

Adjustment – No Disaster Recovery Test Service

This adjustment removes the Disaster Recovery Test Services from the Essential Services Package.

Adjustment – Business Hours Operational Support Coverage

The Supplier should be able to adjust the 24X7 coverage provided in the Essential Services Package and reduce the level of coverage to support the times users are accessing the system. The support hours needed may be 8 or 16 consecutive hours per day across five consecutive business days (Monday – Friday) or seven business days (Monday – Sunday) depending on the location of the user base of the application.

Enhanced Base Package System Support Areas

The systems support services described in this section encompass the Enhanced Packaged Systems Support Services. These services can be expanded with the selection of upgrades for an additional fee or reduced with the selection of adjustments that reduce pricing.

The services provided in the Enhanced Package are designed for dynamic, growing applications that are critical to the Navy's business enterprise.

Systems Management

The Supplier must provide Systems Management Services that include all services defined in the Essential Package plus system DBMS monitoring and printer definition and queue management.

System DBMS Monitoring

Administration and support of a DBMS is divided into two separate areas of responsibility: System Database Support and Application Database Support. System Database Support and Application Database Support functions are differentiated as follows:

- System Database Administration is responsible for managing global DBMS resources that perform functions that require DBMS owner userid authority or functions required to provide overall system integrity for the database (e.g., installation of the DBMS Server software, runtime procedures and parameters for the database instance, creating users and access rights, creating DBMS tablespaces, creating and maintaining rollback and redo logs, etc).
- Application Database Administration is responsible for managing objects within the database (e.g., the Table definitions, indexes, views, procedures etc).

Throughout this document, anytime DBMS requirements are discussed they are directed toward System Database Support and not Application Database Support, which is the responsibility of the program manager.

The Supplier must be able to support Database Management System (DBMS) Monitoring Services that provide the required operational support to monitor the Navy's DBMS environments.

System DBMS Monitoring requirements are:

- The Supplier must monitor DBMS throughput and performance.
- The Supplier must monitor DBMS availability.
- The Supplier must provide a monthly report for DBMS availability as part of the service level management services.
- The Supplier must monitor to detect potential DBMS problems.
- The Supplier must monitor databases for space utilization, database performance, and other specific database criteria such as dead locks.

Note: These support services do not include the services of an application database administrator, but rather the services to maintain the system level components of the DBMS system.

Printer Definition and Queue Management

The Supplier must provide Printer Definition and Queue Management Services that provide the support and processes required to define printers to a midrange system and to manage print queues on a midrange system to resolve problems in the queues through purging and resetting print jobs and queues. Problems are reviewed and actions taken as required in accordance with the problem management procedure. Manual manipulation of print jobs within the queue is not included.

Printer Definition and Queue Management requirements are:

- The Supplier must have a defined printer definition process.
- The Supplier must manage throughput of print queues.
- The Supplier must install and test the printers that are located in the hosted environment.
- The Supplier must resolve problems, including resetting or purging jobs, as needed.
- The Supplier must ensure that applications that print to network printers have the necessary connectivity to the network and that the printer is properly set up on the server. The Supplier must work with NMCI and program management staff to resolve connectivity and reach back problems.

Software Management

The Supplier must provide Software Configuration Management Services that include all services defined in the Essential Services Package plus system DBMS support services.

System Database (DBMS) Support Services

The Supplier must provide System DBMS Support Services that include the processes to plan, install and maintain the required DBMS operating environment to support DBMS software. These support services do not include the services of an application database administrator, but rather includes those services required to maintain the system level components of the DBMS system.

System DBMS Support Service requirements are:

- The Supplier must configure, install, and test DBMS system environment.
- The Supplier must maintain, install, and test DBMS upgrades and patches. All DBMS changes must be presented to the Change Review Board.
- The Supplier must, in coordination with Navy Program Managers, maintain documentation of DBMS configurations including application software release levels, configurations, patches, etc.
- The Supplier must maintain documentation of all changes approved by the Change Review Board including date approved, change summary and date change applied.
- The Supplier must make all documentation available to the Navy upon request.
- The Supplier must create, maintain, and execute DBMS system start-up/shutdown scripts and processes.
- The Supplier must maintain and configure DBMS system disk including slicing and placing.
- The Supplier must create and maintain DBMS files, DBMS tablespace, and application tablespaces.
- The Supplier must verify effectiveness of changes on DBMS files and tablespaces utilizing an approved test plan.

- The Supplier must perform backup and recovery of DBMS system files and tablespaces, as well as the database application itself. Backup schedules and storage requirements are outlined in backup section of the Essential services.
- The Supplier must maintain DBMS Backup/Recovery and Disaster Recovery Procedures and Documentation.
- The Supplier must manage and if necessary modify DBMS file and DBMS tablespace characteristics.
- The Supplier must participate in design reviews and project meetings to provide technical guidance for DBMS related issues.
- The Supplier must work with the Navy Application Program Managers and Navy Technical Application Support Staff to resolve DBMS performance related issues.
- The Supplier must maintain security and access to the DBMS and its associated files.
- DBMS software refresh provides the same services outlined in the software refresh portion of the Essential package.
- The Supplier must work with the Navy's DBA to install application updates or patches.

Workload Management

The Supplier must be able to provide Workload Management Services that include support for Batch Scheduling and Batch Monitoring to determine whether production batch cycles are completed in required time frames.

Batch Scheduling Services

The Supplier must be able to provide Batch Scheduling Services that involve activities associated with defining and maintaining the execution requirements of an application's batch processing that is scheduled under the system's automated scheduling product. The objective of production batch scheduling is that all pre-defined application cycles execute in the proper sequence with cycle completion scheduled realistically within the defined processing windows.

Batch Scheduling Services requirements are:

- The Supplier must maintain the job-scheduling database for the automated scheduling product.
- The Supplier must perform day-to-day maintenance and operational support of the scheduling system.
- The Supplier must perform additions, changes, or deletions to the scheduled batch workload as requested by authorized personnel.
  - The Supplier must assist the Navy Application Program Managers and Navy Technical Support Staff in performing batch scheduling or cycle flow problem determination.

Batch Monitoring Services

The Supplier must provide Batch Monitoring services to support processes necessary to monitor the application batch cycle. If abnormal termination or a restart occurs, the scheduled batch processing will be executed based on pre-defined instructions or the issue will be escalated to the Navy's Application Team as necessary.

Batch Monitoring Services requirements are:

- The Supplier must monitor resource availability, abnormal termination, and cycle start and end times for scheduled batch processing. The Supplier must provide monthly of reports of batch processing statistics to the Navy Program Manager.
- The Supplier must perform and/or assist the application team in performing production batch restarts and reruns.
    - The Supplier must assist the Navy Technical Support Staff in resolving abnormal termination because of system abnormalities.

Note: The Batch Monitoring Services do not include monitoring of the execution of user-submitted jobs.

Application Security and Resource Controls

The Supplier must be able to install any required software tools and set up access parameters and ongoing support required to create and maintain application resource controls for the midrange environment in accordance with the Navy's Application Team requirements.

Application Security and Resource Controls requirements are:

- The Supplier must provide processes to secure application files according to DoN, DoD, and NMCI security requirements.
- The Supplier must manage user access to the applications including the processes and procedures necessary for Adding, Updating and Deleting user access.
- The Supplier must have a process in place to receive and respond to user problems in the areas of file access difficulties and security violations.

Production Promotion

Production Promotion Services include change control services and software for managing the promotion of source and object code for developed programs or applications from test to production environments. This service is designed to make the Supplier responsible for migrating changes into production alleviating the need for Navy Program Managers to perform such tasks. As such the program manager will not need to gain the assistance of the Supplier to gain root access to install an update. The program manager will give the update to the Supplier and the Supplier take all of the steps necessary to install the application update.

The Supplier must provide Production Promotion Services for ongoing maintenance of the hosted applications. These services incorporate procedures for promoting application software changes and application file changes made by the Navy's technical staff into the hosted application's production environment.

Production Promotion Support Services Requirements:

- The Supplier must provide a change control process for source and object code promotion.
- The Supplier should provide version control for source and object code.
- The Supplier must manage the promotion of source and object code from test to model office to production files or server environments.

Customer Support Services

The Supplier must provide Customer Support Services that include request management, change management, problem management, and service level management as they affect the midrange environment. Besides the services provided in the Essential Services Package, the Enhanced Package provides regional coordination of requests.

Request Management – Multi-Site Coordination Services

The Supplier must be able to provide Enhanced Request Management Services that include the coordination of receiving and processing Navy requests for services in a single location as provided in the Essential Services Package, but also regional request coordination. The Supplier must be able to provide request coordination via a single client liaison across multiple regional processing environments that are under the Supplier's control.

This service should integrate software and hardware refresh requests, coordinate scheduling, and provide regional consistency while meeting the Navy's application-specific business requirements. Regional coordination in this context is across multiple sites. When requests requiring this level of coordination are received, the Supplier's request management processes should provide regional communications to coordinate and execute the request among all required locations.

Request Management – Multi-Site Coordination Services requirements are:

- The Supplier should review all requests to determine and understand potential regional requirements and present the findings to the Change Review Board.
  - The Supplier will monitor request status across all impacted regional sites to determine whether deliverables and time frames are met among all environments throughout the region as required. The Supplier will brief the request status to the program manager on a weekly basis.
  - The Supplier will coordinate the scheduling of actions resulting from the request across affected sites.

Enhanced Service – Optional Service Upgrades

The service upgrades can be selected to expand the range of services provided in the Enhanced Services Package based on client-specific requirements.

Upgrade – Custom Product Support

The Supplier will integrate and support a completely customized set of products as defined by the Navy Application Program Managers and the Supplier's Technology Advocate. This set of products should be fully integrated into the operating platform package for installation. Please see the Premier Services Package definition for a detailed list of services.

Upgrade – Local High-Availability Support

The Supplier will support High-Availability Services that provide processes and support for redundant server and storage environments that are clustered together in the same physical site. Please see the Premier Services Package for a detailed list of services included.

Upgrade – Custom Service Level Reviews and Reporting

The Supplier will to provide customized service level reviews and reporting. Please see the Premier Services Package for a detailed list of services included.

Enhanced Services – Optional Service Adjustments

These service adjustments can be selected to reduce the range of services provided in the Enhanced Services Package based on application-specific requirements.

Adjustment – No Printer Definition and Queue Management

The Supplier will remove the Printer Definition and Queue Management Service of Systems Management Services from the Enhanced Services Package.

Adjustment – No Workload Management

The Supplier will remove all Workload Management Services from the Enhanced Services Package. This includes removing support for batch job and cycle scheduling as well as monitoring scheduled batch processing.

Adjustment – No Batch Scheduling

The Supplier will remove the Batch Scheduling Service of Workload Management Services from the Enhanced Services Package. The Operational Monitoring Service for scheduled Batch Processing is not affected.

Adjustment – No System Database (DBMS) Support

The Supplier will remove the System Database (DBMS) Support Service for Software Configuration Management and all monitoring of DBMS from the Enhanced Services Package.

Adjustment – No Production Promotion

This adjustment removes the Production Promotion Service of Workload Management Services from the Enhanced Services Package.

Premier Base Package System Support Areas

The Premier Services Package is designed for Navy's most mission-critical systems that require a customized infrastructure design, build, and operation because of the business application complexity, diversity, and variety. In addition to the services provided in the Enhanced Services Package, the Premier Services Package provides support for more complex software and hardware configurations to provide high availability for business critical processing requirements.

Systems Management

Systems Management is the process of analyzing, evaluating, and reviewing the compute operation to verify that operational requirements are met. The range of services includes all services defined in the Enhanced Services Package plus Application Monitoring and advanced web site monitoring.

Application Monitoring

The Application Monitoring Service provides the Navy with proactive automation and monitoring that result in more stable, functional applications that meet Navy and operational requirements. Application monitoring involves more than the monitoring of application resources. Application monitoring can involve monitoring distinct functions within the application for input/output speed, checking for looping/hung processes, analyzing application usage patterns (which options or branches are used most often), and reviewing exception logs.

This service is designed for monitoring purposes only. Program manager cooperation may be required to interface monitoring agents with the application code.

Application Monitoring Services Requirements are:

- The Supplier must develop, install, and test specific application automation agents for use in application monitoring.
- The Supplier must configure, install, and test custom product automation agents.
- The Supplier must manage and monitor the application and/or custom product operational environment.
- The Supplier should monitor the application database to ensure the database is responding to requests if applicable.

Web Site Monitoring

The Web Site Monitoring Service provides the Navy with automated monitoring of web sites to ensure there are no broken links in the Web Site. A broken link is defined as a hyperlink from one web page to another that is no longer available.

Web Site Monitoring Services Requirements are:

- The Supplier should monitor identified web pages for broken links on a periodic basis as defined by the Navy Program Manager.
- The Supplier should provide results of broken links to the Navy Program Manager.

Software Management

Software Configuration Management Services provides for the installation, maintenance, documentation and upgrading of midrange environments. The range of services includes all services defined in the Essential and Enhanced Services Packages plus Custom Product Support and Local High-Availability Support Services.

Custom Product Support

The Supplier must integrate and support a completely customized set of products (operating systems, network devices, server hardware, etc.) as agreed upon by the Navy and the Supplier. Custom products in this context refer to support for nonstandard software or hardware that is utilized by the application. Operating systems such as Linux or BSD UNIX are nonstandard, and the contractor may have to hire additional personnel to support the software. Custom support does not refer to the application itself.

Custom Product Support Services Requirements are:

- The Supplier must support a custom-designed solution of system-related vendor products selected by the Navy and the Supplier.
- The Supplier must plan, install, integrate, and upgrade the custom product set.
- The Supplier must resolve problems, including problem determination, interface, and escalation with third-party suppliers, for the custom product set.
- The Supplier must install corrective and preventive maintenance to custom product sets.
- The Supplier must conduct inventory, track, and document the custom product set components and changes.
- The Supplier must provide software refreshes to allow early adoption or to maintain currency to current software versions of the custom product. Software refresh may not be applicable in some cases where the custom product is being used because of hard coded dependencies specific to a particular version.

Local High-Availability Software Support

Local High-Availability Software Support Services provide the processes and support staff to support system software required to provide redundant server and storage configurations clustered together in the same physical site.

Local High-Availability Support Services Requirements are:

- The Supplier must install and maintain the system software and related tools required to provide a midrange compute environment that meets availability requirements and removes single points of failure from the compute configuration.
- The Supplier must provide high-availability software expertise to manage and monitor the operational environment.
- The platform will support non-disruptive software maintenance to both the system software and the application

Hardware Configuration Management

The Hardware Configuration Management of the Premier Services Package includes the processes and procedures for the installation, upgrade, coordination and oversight of midrange high-availability environments. The range of services includes all services defined in the Enhanced Package plus hardware refreshes as required to maintain state-of-the-art high availability configurations.

Local High-Availability Hardware Support

Local High-Availability Hardware Support services provide the processes and support for redundant server and storage configurations that are clustered together in the same physical site to support continuous availability requirements.

Local High-Availability Hardware Support Services Requirements are:

- The Supplier must manage platform solution configuration requirements to meet availability requirements and remove single points of failure from the compute configuration.
- The Supplier must provide subject-matter expertise to manage and monitor the operational environment.
- The Supplier must coordinate with vendors to provide non-disruptive maintenance processes.
- The Supplier must provide the capability to dynamically reconfigure resources to support applications experiencing high demand.

Customer Support Service

The Supplier must be able to provide Customer Support Services that include a more extensive range of Change and Problem Management Services. The complete set of services that are provided encompass all services defined in the Enhanced Package and additional client-specific change and service reviews.

Request Management – Global Coordination

Premier Request Management Services include not only the coordination of receiving and processing Navy requests for services within geographic regions as provided in the Enhanced Services Package, but also global request coordination. The Premier Services Package must provide request coordination via a single Supplier client liaison across all global processing environments. This service integrates such services as software and hardware refresh requests, coordinates scheduling, and provides global consistency while still meeting client-specific business requirements. When requests requiring this level of coordination are received, Supplier request management processes provide the global communication to coordinate and execute the request among all required locations.

Request Management – Global Coordination Services Requirements are:

- The Supplier must review all hardware and system software requests to determine and understand potential global requirements.

- The Supplier must communicate and monitor the status of the request across all impacted global sites to ensure deliverables and time frames are met among all global environments as required.

Custom Service Reviews and Reporting

Custom Service Reviews and Reporting includes additions to Standard Service Level Management Reviews and Reporting. Navy-specific service level reporting must be available and customized to address unique reporting requirements. The review and reporting services for change and problem management can be customized to meet application specific requirements. More frequent problem and change management review services that encompass weekly Navy-specific problem review meetings and daily service review meetings for all problem metrics are also provided.

Premier Services – Optional Service UpgradeUpgrades

The service upgradeupgrades can be selected to expand the range of services provided in the Premier Package based on program-specific requirements. There is an additional charge associated with each service upgrade.

Upgrade – Remote High-Availability Support Services

The Supplier must have Remote High-Availability Support Services that provide the processes and support for redundant server and storage configurations that are located in geographically distributed physical sites either via hardware and/or software tools to support specified availability requirements. Besides the protection provided by a local high-availability solution, a remote high-availability configuration provides business continuity if the local operating site is incapacitated.

The components of a remote high-availability configuration include remotely clustered platform configurations and remote mirrored disk storage configurations. When redundant sites are requested, the Supplier and the solution vendors perform a risk/cost/benefit analysis for Navy approval. Eliminating single points of failure helps prevent interruptions in service because of discrete hardware and software failures.

Remote High-Availability Support Services Requirements are:

- The Supplier must design and implement a configuration to meet availability requirements and remove single points of failure from the compute configuration.
- The Supplier must provide subject-matter expertise to manage and monitor the environment as defined by the services selected for the application.
- The Supplier must coordinate vendors to provide non-disruptive maintenance processes to ensure the availability of the hardware components of the compute configuration.
- The platform configuration must allownon-disruptive system and application software maintenance to ensure the availability of the software components of the compute configuration.

Premier Services – Optional Service Adjustments

These service adjustments can be selected to reduce the range of services provided in the Premier Package based on client-specific requirements. There is a price reduction associated with each service adjustment.

Adjustment – No High-Availability Support

This adjustment removes local High-Availability Services from the Premier Package. This includes removal of local High-Availability Services that provide the processes and support staff to support redundant server and storage configurations that are clustered together in the same physical site either via hardware and/or software tools to support continuous availability requirements.

Adjustment – No Request Management – Global Coordination Support

This adjustment removes Request Management – Global Coordination Services from the Premier Package.

Contract Termination

At the conclusion of the contract, the Supplier must assist the Navy Program Manager and any third party contractor in migrating the application to a new environment. This includes allowing a third party contractor access to the servers to evaluate the applications. The Supplier must perform the following actions upon the completion of the contract:

- Transfer the application or groups of applications to a suitable media for transport to the new environment.
- Provide software and hardware configuration information.
- The Supplier must provide audit information to assist any third party organization in gathering data necessary to migrate the application.
- The Supplier must turn over all application related backup disks.
- The Supplier must purge all application data from their systems in accordance with DoD and DoN regulations.
- The Supplier must provide all required end-of-month reports and documentation.

Acknowledgements

The author would like to acknowledge the assistance of Scott Price and Joseph Vickery from EDS. Their contributions throughout this paper, especially in the facilities portion of this paper, were invaluable.

Appendix A:
N/MCI Contract N00024-00-D-6000 Attachment 4 Security Requirements Section 1.1.4

1.1.4 Contractor Specific Internal Information Guidelines

1.1.4.1 Classified (DoD) Information Support

The highest classification level of information required in connection with this procurement is TOP SECRET.

In accordance with the National Industrial Security Program Operating Manual, DoD 5220.M, the contractor shall possess or be able to possess a Facility Security Clearance equal to the highest level of classified information necessary to perform the tasks or services required on this contract.

Contractor personnel, whose duties require access to systems processing classified information, shall possess a security clearance at least equal to the highest degree of classification involved and shall have a validated need-to-know prior to beginning work on the classified system.

The sponsoring agency security requirements for classified systems shall be met by all contractor personnel accessing classified information, or contractor systems processing classified information.

The contractor shall perform internal assessments to determine position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes, such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges at contractor facilities. These position sensitivity assessments will be forwarded to the Government for a determination of personnel suitability and requirements for individuals assigned to these positions in accordance with DRD3. Periodic re-evaluations of positions and suitability requirements will be necessary during the life of the contract as positions and assignments change.

The contractor shall conduct risk assessments, document the results, develop and maintain internal security plans. These plans shall describe how the contractor ensures the integrity, availability, and confidentiality of the information that it is operationally responsible to protect within the vendor's facilities.

1.1.4.2 Sensitive Information Support (Non-classified)

Under current Federal guidelines, all officially held information is considered sensitive to some degree, and shall be appropriately protected by the contractor as specified in applicable IT Security Plans.

Types of sensitive information that will be found on DoN systems that the contractor shall have access to include, but are not limited to: Privacy Act information; proprietary information of other companies or contractors; resources protected by International

Traffic in Arms Regulation (ITAR); technology restricted from foreign dissemination for competitive reasons; DoN administrative communications, including those of senior government officials; procurement or budget data; information on pending Equal employment Opportunity (EEO) cases; labor relations; legal actions; disciplinary actions; complaints; IT security pending cases; civil and criminal investigations; information not releasable under the Freedom of Information Act (FOIA) (e.g. payroll, personnel, and medical data).

The contractor shall perform internal assessments to determine position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes, such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges at contractor facilities. These position sensitivity assessments will be forwarded to the Government for a determination of personnel suitability and requirements for individuals assigned to these positions. Periodic re-evaluations of positions and suitability requirements will be necessary during the life of the contract as positions and assignments change.

The contractor shall conduct risk assessments, document the results, develop and maintain internal security plans. These plans shall describe how the contractor will ensure the integrity, availability, and confidentiality of the information that is operationally responsible to protect within the vendor's facilities and at government facilities. For example the contractor shall ensure that foreign nationals within their corporate staff will not have access to NMCI data that is not releasable. A decision to accept any residual risk will be the responsibility of the DoN system owner and the DoN information owners. The contractors risk assessments and IT Security Plans shall be updated at least every three years or upon significant change to the functionality of the assets, network connectivity, or mission of the system, whichever comes first. If new or unanticipated threats or hazards are discovered by the contractor, or if existing safeguards have ceased to function effectively, the contractor shall update the risk assessments and IT Security Plans (within 30 working days) and shall make appropriate risk reduction Recommendations to the DoN system owner and the DoN information owners (within 5 working days).

1.1.4.3 Privacy And Security Safeguards

The contractor shall not publish or disclose in any manner, without written consent of the government, the details of any security safeguards designed, developed, or implemented by the contractor under this contract or existing at any DoN Center.

The contractor shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) is cleared of all DoN data and sensitive application software by a technique approved by the government. For IT resources leaving DoN use, applications acquired with a "site license" or "server license" shall be removed. Damaged IT storage media will be degaussed and destroyed.

To the extent required to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of government data, the contractor shall afford DoN access to contractor facilities, installations, technical capabilities, operations, documentation, records, databases, and personnel.

NAVSUP Service Level Agreements

Service level agreements have many formats depending upon how they are used. Internal SLAs between management and the IT department can be more informal because many of the procedural issues are stated elsewhere. SLAs involving external service providers need to be more formal.

SLAs serve as a mechanism to notify all parties of services that will be performed, performance expectations, responsibilities of all parties, penalties for non-performance, and SLA resolution procedures. SLAs also define the oversight and interaction between the program managers and the service provider.

SLAs are often used in conjunction with a Statement of Work (SOW), which provides the actual requirements. The SLAs provide the metrics to measure whether the requirements are being met. Most activities find it easier to keep the two documents separate, as many requirements will not have SLAs associated with them.

The following is the SLA template that NAVSUP will be utilizing:

Service Name: This is the name of the service category that is being measured (e.g., help desk support).

Service Description: This is a detailed discussion of the service that is to be performed. This represents the business function, process, or procedure that is to be measured.

Reason for Measuring: This section should provide the rational for this SLA. A valid justification prevents measuring for measurement sake. The results of the measurement should result in problem determination, lead to corrective action, and maintain the performance achieved by the corrective action. The SLAs should be linked to a strategic or tactical business concern.

Time Frame: This is the time period during which measurements are taken (e.g., 24x7x365, or from 0700-1900 Monday through Friday)

Scope: This section defines where the services apply (e.g., this applies to the system software only). This section also provides amplifying information such as categorization of problem calls (i.e., priority 1 equates to an emergency), and information necessary to ensure all parties understand the areas that are covered by the SLA. The scope also details areas not covered by the SLAs.

> **Performance Category**: This section names sub-services that must be measured to determine the over-all efficacy of the service. There can be numerous performance categories associated with one SLA. The following subsections are associated with every performance category:
>
> **Performance Metric**: This section describes the metric to measure performance.
>
> **Threshold Levels**: This section describes the performance thresholds that must be met at the various service levels. There are generally more than one level of service. In the example that will be presented, three service levels will be used. Obviously as the thresholds become more difficult to meet, the costs of providing the service will rise.
>
> **Formula**: The formula describes how the metric will be computed.
>
> **Assumptions**: All assumptions should be stated in this section.
>
> **Contractor Responsibility**: This section details the contractor's responsibilities in meeting the service level requirements.

Customer Responsibility: The program manager or the end-user's responsibilities are outlined in this section (e.g., a trouble call must be initiated before metrics covering the help desk can apply).

Frequency: This is the period of time over which measurements will be taken to determine SLA compliancy (e.g., monthly, quarterly). This usually equates to the periodicity of the reporting requirements.

Measurement Techniques: How will the metrics be gathered? This describes the procedures that will be used to collect the performance measurements.

Reports Required: This section details the reports required from the service provider to verify actual performance against SLA thresholds. It also details the periodicity requirements of the reports (e.g., Trouble Tickets – Monthly). The person reviewing the SLAs may have access to the report generating tool, and can manipulate the reports as needed. An example is if the reviewer has online access to the trouble tickets, that individual can do daily, weekly or monthly reports, at whatever level of abstraction is needed.

The specific reports required will be outlined in the Contractor Data Requirements List (CDRL), which is separate from this SLA. The CDRL will detail the format and content required, the frequency, distribution, and means of dissemination. The reports required will vary depending upon the type of application, the criticality of the application, monitoring tools used, funds available, and management needs. Typically daily reports are more technically oriented and are used by the CTR for verification; weekly or monthly reports are generally aggregate reports that provide service level summaries to management.

Person Responsible for Verification: This section details who will be reviewing the SLA measurements and determining compliancy. In the government, this person is usually the Contracting Technical Representative (CTR).

Escalation Procedures: This section describes actions to be taken when thresholds are exceeded, and who should be notified. For example if help desk response time is 15 minutes for a critical application, and 30 minutes have passed, who should be notified? This also includes situations where thresholds are violated on numerous occasions throughout the reporting period. This section also describes escalation procedures if the CTR and service provider cannot agree that a threshold violation has occurred.

Contractual Exceptions: This section describes the exceptions to the SLA. For example an emergency situation may require the service provider to violate a SLA threshold.

Penalties/Rewards: An SLA without penalties or rewards is nothing more than an agreement. SLAs must have a mechanism to enforce compliancy. This section describes what action will be taken if thresholds are violated, or if SLAs are met. It is important to identify minor and major thresholds to ensure that the service provider is taking action to correct the problems.

Service Name	SLA 1.0: Compute Service Availability
Service Description	Availability measures the capability of an end-user to access and fully utilize an application (according to specifications) over a period of time. Availability is usually expressed as a percentage of time that the system was available for use divided by the agreed upon hours of operation. The time period that an end-user cannot utilize the application is considered 'downtime'. Availability metrics are generally intended to be end-to-end, reflecting availability from the end users perspective. However, these SLAs only cover the host environment, so availability metrics will be restricted to the host environment only, and will not apply to the client piece or the connectivity from the client to the host environment firewall. Downtime can also be difficult to define. This SLA will concentrate on an application's opportunity to compute. The thresholds will contain metrics to ensure that the application has sufficient resources to operate to specifications. If the compute environment is not operating at a certain level of efficiency, the application performance suffers. As a result, if certain resource thresholds are not met, the period of time the resources do not meet the thresholds will count as downtime. Response time is another element of availability that must be addressed. The SLA is limited to the host environment, so application response time will be calculated from the time a server receives application input until it provides the correct output. It is necessary to develop a program that resides on the server in order to generate the information necessary to measure response time (this is often referred to as synthetic transactions). The program will test key application functionality at random times and measure the response time from when the input is initiated until the desired output is correctly received. Response times will apply to enhanced and premier services only. It is assumed that the government will develop the synthetic transaction software. Development of the program will be negotiated as a separate line item if the program wants the service provider to perform that function.

Reason for Measuring	Availability is a measure of quality. The program manager and the contractor need to constantly monitor the infrastructure, hardware and system software to measure the effectiveness of the hardware and software in supporting the application. Diligent monitoring will detect early signs of problems that may require maintenance action. The efficacy of the application support has direct business impacts. When the application is not available any business related to that application stops; opportunities are missed, business processes are impacted, and deadlines can be missed. The program manager must identify a target availability threshold and be able to justify expenses associated with it. This will involve determining the business impact of lost service. The contractor must evaluate the infrastructure to determine if it is possible to support the availability, or if redesign or additional redundant or high availability equipment is needed. The host environment cannot be designed, implemented, or managed unless an availability threshold is established.
Time Frame	Derived by the contracted number of support hours. The Default is 24x7x365. Scheduled maintenance time that is within the maintenance window, and does not exceed the agreed upon maintenance time frames will not be included in availability computations. Additionally, scheduled maintenance involving the application (i.e., granting root access to maintenance personnel to perform an upgrade) will not be considered down time. The Maximum "Available" time will be determined from the hours of support that were contracted. Example (1): Hours of Support = 24 x 7. The maximum "available" time in a 30 day month is 30 x 24 x 60 = 43,200 minutes. Example (2): Hours of Support = 9 x 5. The maximum "available" time in a month with 21 work days is: 21 x 9 x 60 = 11,340 minutes.
Scope	This is an end-to-end metric from the host environment firewall to the application. It includes the hardware and

	the software for the firewall and server farm network, in addition to the hardware and software necessary to support the application. It does not apply to the application itself.

Performance Category	1.0 Host Environment Availability
Performance Metric	Availability is expressed as a percentage of the time that an application is fully functional divided by the total time encompassed in the support hours.
Threshold Levels	Availability thresholds are as follows: Essential Services: 99.50% Enhanced Services: 99.90% Premier Services: 99.95% In this SLA, availability is not only dependent upon the individual components that comprise the infrastructure (servers, network and firewall); it also addresses application and data availability from a security perspective. The following thresholds apply to resource utilization and network efficiency. If these thresholds are violated, then the application is considered 'down', and will count against availability: Server Measures: CPU Utilization: 75% sustained for over 1 hour. Not to exceed 90% for more than 2 polling cycles (5 minute intervals). Frequency of Failure: More than 3 service interruption in one day. Disk Utilization: 90% Disk Response Time: .25 second Disk Average Queue Length: 3 Disk I/O rate: 100 ms average Swap space availability: 90% of defined space Memory paging: 5 per second Network Measures: Data Delivery Rate: 99.95% LAN Latency (one way): 70 ms LAN Packet Collisions: More than 7% of packets transmitted (average based on a 1 hour interval). Bandwidth Availability: 85% of defined bandwidth Ethernet Segment Utilization: Less than 30% Security Related Measures: If application performance is degraded due to an intruder attack, virus, worm, or security breaches previously identified, the application is considered "down". This

	includes the time that the application is affected during efforts to correct the violation. New attacks that have no previous history or signature will not be counted as "down time" against availability as long as the attacks did not exploit vulnerabilities that were corrected by security patches that should have been installed. Application Response Time: Will be dependent upon the types of transactions that are being performed. If all transactions are similar, one threshold value can be determined (e.g., query requests must be generated and returned within 1 second). If the transaction response times vary considerably, the response thresholds should be specific to the transaction. In this SLA, response times are generated from synthetic transactions and are measured from the server only. All hardware errors affecting the application are considered 'downtime', and will be counted against availability.
Formula	Availability = (total uptime minutes) / (total uptime minutes + total downtime minutes) * 100
Assumptions	Downtime starts with the generation of a trouble ticket, or when the monitoring tools capture a threshold violation. Problems relating to the firewall, network, server or system software will count towards downtime. A review of the trouble tickets and monitoring software reports will verify that the downtime is properly assigned. Downtime attributed to application errors will not be included in the computation. Downtime that is a direct result of government actions will not be included in the computation. An example would be rebooting the system following an application update. Errors attributed to the client side portion of the compute environment will not be charged against reliability calculations.
Contractor Responsibility	Adopt and implement an industry-standard software solution for automatically polling and calculating compute service availability. Monitor compute services for earliest identification of outages. Take appropriate actions to correct deficiencies.

Customer Responsibility	The customer is responsible for prompt notification of any suspected compute service outages.
Frequency	Monitoring is conducted during scheduled support hours. Report frequency is monthly. Assigned government representatives will have real-time or near real-time access to monitoring software (read-only mode is acceptable).
Measurement Techniques	The server will be ’Pinged‘ from a management server every 5 minutes. Failure by the server to respond will start the service outage time. The time between the first ’Failed‘ Ping and the first successful Ping after repair will be reported as Downtime. Example: Server A polled at 10:40, 10:45 and 10:50 and does not respond to the 10:45 poll but does respond at 10:40 and the 10:50. This would be calculated as 5 minutes of downtime. Approved industry standard monitoring tools such as Tivoli® and Open View® will be used to monitor the server and network. Operating system logs will also be used to determine compliance. Threshold violations will be considered downtime. Each threshold specified will have to be evaluated to determine the period over which the measurement is determined. Unless otherwise specified, thresholds that specify averages will be computed over a 1-hour period. Other thresholds will normally be monitored in real-time, or near real time. "Down time" is considered when a threshold is violated for more than 5 minutes. The downtime will be reviewed and adjusted by a contractor representative to exclude all outages from maintenance windows or outside the scope of service: • All planned outages • All outages due to application failures Adjusted Compute Service Availability is then recalculated. The new formula would be as follows: Availability = (total uptime minutes – downtime outside of scope) / (total uptime minutes – downtime outside of scope + total downtime minutes) * 100 Example Calculation: Server contracted for 7 x 24 hour support. Two outages occurred during a month with 30 days: (1) 100 minute

	application outage and (2) a 360 minute system failure occurred for a total downtime of 460 minutes. Availability is reported as: Reliability = (43,200 – 100) / ((43,200 – 100) + 360) * 100 = 99.17%
Reports	1. Monitoring reports: Weekly, in addition to real-time/near real time viewing of the monitoring tools that will allow visibility to raw data. 2. Trouble tickets: Weekly
Person Responsible for Verification	The Contractor Technical Representative (CTR) will be responsible for reviewing the monitoring reports and trouble tickets to determine compliance with the SLAs.
Escalation Procedures	The CTR will be notified if the application is not accessible or functioning by the following time frames: Essential Service – after 30 minutes Enhanced Service – after 15 minutes Premier Service – after 10 minutes If there are any disagreements concerning whether downtime should be charged to the application, or the host environment, the CTR will make the decision. Disagreements can be escalated to the Contracting Officer Representative (COR).
Contractual Exceptions	Availability does not include scheduled maintenance downtime within the maintenance window.
Penalties/Rewards	Minor penalty: 10% of monthly rate • Threshold values exceed agreed upon rates. Major violation: 25% monthly rate • More than 3 minor penalties during the year • Any availability less than the following: Essential Services: 98.0% available Enhanced Services: 99.0% available Premier Services: 99.5% available • More than 2 major violations will force escalation procedures between the COR and the contractor. Following escalation procedures additional missed targets may be cause for termination.

Service Name	SLA 2.0: Restoration of Service
Service Description	Restoration of Service involves the implementation of procedures that ensure critical business operations resume following a disaster and that they return to normal as soon as possible. Service restoration is part of an organization's COOP plan.
Reason for Measuring	Restoration of Service is measured to ensure that systems can meet the recovery times and resume full operations within acceptable time limits based on the criticality of the application.
Time Frame	The time frame of measurement is from the time that the application is no longer available until the application is fully restored (operating in accordance with SLA defined performance criteria).
Scope	Restoration of Services applies to all of the components (hardware and software) that are required to access and run the application.

Performance Category	2.0 Restoration Time
Performance Metric	The metric used to measure compliance with restoration services is the amount of time from when services were terminated to when the end user can access and fully utilize an application.
Threshold Levels	The thresholds are as follows: Enhanced: Less than 5 days Essential: Less than 48 hours Premier: Less than 4 hours Premier with Remote High Availability: Less than 15 minutes
Formula	The amount of time from the initial disaster report until the application can be accessed and utilized to its full functionality by an end-user.
Assumptions	The contractor will notify the CTR and program manager as soon as possible after a disaster occurs. Help desk personnel should also be notified so they can inform users reporting problems with the application.
Contractor Responsibility	The Contractor must work with the Program Manager's staff to help define the recovery requirements and then to document the procedures for the Resumption of Service for the system in a Disaster Recovery Plan. The Contractor must test the Disaster Recovery Plan for the systems annually and provide a summary of the test to the CTR.

	The contractor must have accurate, timely hardware and software configuration data as well as application and system software implementation procedures.
Customer Responsibility	The Program Manager must define the level of criticality of the application being hosted and work with the Contractor to define the Disaster Recovery Requirements. The Program Manager must ensure that any government employees needed to restore an application be available in the event a disaster occurs and that they participate in the annual testing. In the event that government personnel are not able to assist in the application recovery efforts, the program manager is responsible for providing loading instructions and test scripts to ensure that the application is functioning correctly after the application is installed in the new environment.
Frequency	Disaster recovery will be tested annually. This SLA will apply when a disaster occurs.
Measurement Techniques	The Resumption of Service is measured by adding the total minutes that it takes from the time a disaster is recognized as having occurred (defined as the time that service was no longer available) to the time the system has resumed business operations (defined as services are resumed to full SLAs). The CTR will check with the help desk to determine if a trouble ticket has been opened for the applications affected by the disaster. If a trouble ticket has been opened, the CTR will use that trouble ticket as a start time for measuring the time of disaster. If a trouble ticket has not been opened, the CTR will initiate the trouble ticket for the application(s). The Service Provider will notify the CTR when the applications are ready for operation (this assumes the application was tested using the test scripts). If test scripts were not available, any time between when the application is available for testing and the time that the program management staff performs a functional test of the application will not be held against the Service Provider unless the tests fail. The trouble ticket should be closed after resumption of operations.
Reports	1. Disaster recovery test results 2. Disaster recovery plan

	3. Trouble tickets
Person Responsible for Verification	The CTR will be responsible for determining a time when the application was not available due to a disaster, and when services were resumed to SLA defined standards.
Escalation Procedures	If services exceed thresholds, the CTR will be notified.
Contractual Exceptions	None
Penalties/Rewards	Minor penalty: 5% of monthly rate • Threshold values exceed agreed upon rates. Major Penalties: 25% of monthly rate • Restoring services violated thresholds by more than 20%. • 5% of monthly rate will be penalized for each day after a major penalty is assessed. The CTR and program manager have the discretion on whether to apply any penalties.

Service Name	SLA 3.0: Help Desk Service Reporting
Service Description	The help desk is the central point of contact for problem resolution. If a customer is experiencing any problems, or needs to request services, they must contact the central help desk for assistance. The help desk will either resolve the problem while they are on the phone, or they will generate trouble call tickets to assign the problem or task to the appropriate point of contact. Under the Navy/Marine Corps Intranet (NMCI), the Navy has outsourced personal computers and infrastructure to EDS. As a result any end-user problems will start with the NMCI help desk. If the problem appears to reside within the host environment, the NMCI help desk will pass the trouble ticket to the contractor's help desk.
Reason for Measuring	The help desk is the central point of contact for problem resolution. They are the direct interface to the end-user. The help desk collects metrics needed to identify problem areas, and to provide the quality assurance that is needed to ensure that customers are supported. The trouble tickets that are generated indicate problems that may extend beyond a single caller. Prompt response by the help desk may avert more problems. The help desk not only collects information on problems through the generation of trouble tickets, but they also provide an initial resolution to problems by answering questions, or guiding users through procedures. Help desk performance must be measured to ensure the end-users are receiving the support they require, trouble tickets are being accurately generated, and action is being taken to let users know the status of their trouble tickets. Trouble tickets are one way to measure availability. It is possible that a server and application are operating within established performance thresholds, but the aggregate of the various components are affecting the performance of the application. The end-user can contact the help desk to report the application's poor performance.
Time Frame	Help Desk service will be measured during support hours. The default is 24 x 7.
Scope	Under NMCI, the help desk will take the initial call, and will pass a trouble ticket to the contractor help desk if the problem does not involve the client piece of the

	application, or the client side of the infrastructure. The help desk at the host environment will take the appropriate action to resolve the problem. This SLA applies to the contractor's help desk, and does not include any actions taken by the NMCI help desk. Thresholds will be based on direct phone calls or e-mails, and trouble tickets (or similar measures) passed from the NMCI help desk. The contractor's help desk is responsible for contacting the individual submitting the trouble call if additional information is needed. The help desk is also responsible for providing feedback on efforts to fix the problem, and to provide an estimated problem resolution time. When the problem is resolved, the help desk will close out the trouble ticket. In some cases the contractor's help desk will service requests directly from the CTR, ISSM, program manger's staff, and software developers/maintainers. The vast majority of telephone calls will be for services, instead of reporting problems. Most problem calls are initiated by the end-user, and they should initially be routed through the NMCI help desk. Software exists that can monitor every incoming call to determine an average time to respond, dropped call rate, time on hold, and average length on time responding to callers. Unfortunately this software is very expensive. If the contractor already has this software, then metrics can be revised to take advantage of that monitoring capability. However since the NMCI help desk will field most calls, the cost to collect these metrics is not justified. Instead the help desk metrics in this SLA will concentrate on the response to the passed trouble tickets and the response to phone calls will be based on surveys taken from end-users.
Performance Category	3.0 Help Desk Availability
Performance Metric	This is a measurement of the availability of the help desk to respond to requests or problems. The metric used will be the probability expressed as a percentage that the help desk will answer a call, or receive and process a trouble ticket passed from the NMCI help desk.
Threshold Levels	The following are the thresholds for help desk availability: Essential - Premier: 99%

	Automatic answers to voice mail are not acceptable for contractor help desk operations.
Formula	The formula will consist of dividing all phone calls, e-mails or passed trouble tickets that the contractor's help desk has taken action on divided by the total calls, e-mail or trouble tickets sent to the contractor's help desk.
Assumptions	The NMCI help desk will be able to pass trouble tickets to the contractor's help desk. The NMCI help desk software is Remedy. The contractor's help desk must be able to interface with Remedy©, or another method of passing the trouble tickets will have to be developed and approved by the government.
Contractor Responsibility	The contractor should have a system to ensure that trouble tickets passed from the NMCI help desk are received by the contractor's help desk.
Customer Responsibility	If the end-user is experiencing problems with an application, the problem needs to be routed through the NMCI help desk. The contractor's help desk will primarily respond to trouble tickets from the NMCI help desk and phone calls requesting hosting specific services.
Frequency	Monthly
Measurement Techniques	The total trouble tickets sent from the NMCI help desk to the contractor's help desk will be gathered from the NMCI help desk software. Tickets received will be gathered from the contractor's help desk software. The measurement of phone calls answered will be gathered from interviews and spot checks by the CTR.
Reports	1. Trouble tickets from the NMCI help desk 2. Trouble tickets from the contractor's help desk
Person Responsible for Verification	The CTR will verify the contractor's help desk availability.

Performance Category	3.1 Initial Feedback
Performance Metric	This is the period of time from submission of the trouble call until the caller is notified that a trouble ticket has been filled out, and an estimated completion time is given. Feedback is generally provided in the form of an e-mail with the information that is contained on the trouble ticket. This allows the caller to verify that the information on the trouble ticket is correct, and it provides the caller with an anticipated resolution time. The feedback must also categorize the problem and provide the agreed upon resolution time frames.
Threshold Levels	The following are the thresholds for initial feedback:

	Essential - Premier: Less than 15 minutes
Formula	Time trouble ticket is completed minus the time the e-mail is sent. Measurements are in whole minutes. For example, if the trouble ticket was finished at 10:20am and the e-mail was sent at 10:29, then the time period was 9 minutes.
Assumptions	The help desk software program must have the capability to e-mail the caller the trouble ticket, or the e-mail of the end-user reporting the problem must be contained in the trouble ticket passed from the NMCI help desk.
Contractor Responsibility	When feedback is provided to the caller, a copy of the e-mail should be sent to the CTR.
Customer Responsibility	If there are problems with the trouble ticket as it was passed, or if the end-user disagrees with the categorization of the problem, the end-user needs to respond to the e-mail outlining the issues. A copy will be sent to the CTR. If the CTR disagrees with a categorization of the problem, the CTR needs to contact the contractor and resolve the issue.
Frequency	The data will be gathered over the period of 1 month.
Measurement Techniques	The CTR will utilize the feedback e-mails to determine the time periods of the feedback.
Reports	1. Trouble tickets 2. E-mails received from the contractor's help desk
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	3.2 Repeat Problems
Performance Metric	This is a measurement of the accuracy with which problems are resolved. When a trouble ticket is closed out, the problem should be investigated and corrected. Repeat problems are those problems that have been reported via a trouble ticket that have occurred again within 30 days from the close out of the trouble ticket.
Threshold Levels	The following are the thresholds for repeat problems: Essential - Premier: 05% Problems that reoccur within a 30-day window will be counted against the month in which the problem reoccurred.
Formula	Number of repeat trouble calls divided by total trouble calls. For example if 5 trouble calls had to be reworked, out of a total of 100 trouble calls, the formula would be as follows: (5/100)*100 = 05%
Assumptions	In some cases the problem will require in-depth problem analysis. Rebooting the system will not allow a root determination of the problem.

	The program manager and the contractor will determine when in-depth analysis should be performed. If the program manager is reluctant to perform in-depth analysis, and is comfortable with rebooting the system to solve the problem, then the CTR after receiving concurrence from both parties will not count those faults towards this SLA.
Contractor Responsibility	The contractor needs to notify the program manager when there appears to be a recurring problem that cannot be solved without in depth trouble shooting.
Customer Responsibility	When recurring problems are occurring, the program manager needs to make the determination on whether they need to conduct in-depth root cause analysis when the next fault occurs.
Frequency	Every quarter.
Measurement Techniques	The CTR will receive copies of the trouble call feedback e-mails, which can be used to determine reoccurring problems. In addition interviews with program management staff and end-users will be conducted to determine if the root cause for different problems are the same.
Reports	1. Trouble ticket feedback e-mails 2. Monitoring tools
Person Responsible for Verification	The CTR is responsible for verification.
Escalation Procedures	Issues will be brought to the attention of the CTR. The CTR can escalate the issue to the COR if it cannot be resolved at the CTR level.
Contractual Exceptions	Problems that require in-depth analysis will be excluded from the total of reworked trouble tickets. This exclusion will require concurrence from the contractor and program manager.
Penalties/Rewards	Minor penalty: 5% of monthly rate Threshold values exceed agreed upon rates. Major Penalty: 15% monthly rate • 3.0 Help Desk Reliability Essential - Premier: Less than 95% • 3.1 Initial Feedback Essential - Premier: Less than 45 minutes • 3.2 Repeat Problems Essential - Premier: 10% Penalties will be levied at the discretion of the CTR.

Service Name	SLA 4.0: Problem Resolution
Service Description	Problem resolution measures of the contractor's ability to identify, respond, and correct problems or issues that affect compute services.
Reason for Measuring	Problem resolution is a portion of the mean time to repair (MTTR), which factors into overall availability. This has a direct impact on the end-user's ability to utilize the application. If the occurrence of problems remains constant, a lower MTTR will increase the operational availability of the application. Problem resolution is an important metric in measuring customer support. It measures the contractor's response time to resolving issues, as well as the skill at which they apply long-term solutions.
Time Frame	Derived by the selected hours of support. The default is 24 X 7.
Scope	This SLA measures the resolution time frames for problems reported to the contractor's help desk, or detected by monitoring software. The SLA applies to problems within the host environment. Problems are defined as a change of state in the software, hardware, or infrastructure within the host environment that adversely affects the performance of the application. Hardware or software errors that do not affect the application's performance or functionality will not be included in this SLA. The contractor will be held responsible for the resolution time on any third party hardware or software that is residing in the host environment. Problem resolution does not include problems that can be corrected by the contractor's help desk during the initial trouble report. Problems associated with the client side computer or infrastructure will be passed to the NMCI help desk, and the NMCI SLA will pertain. Problem resolution applies to the firewall, infrastructure, hardware, and software in the host environment, except the application software. Problems relating specifically to the application will be passed to the appropriate application point of contact and will not be within the scope of problem resolution.

	Priority 1 issues: Mission Critical Impact: Priority 1 issues involve critical component failure resulting in loss of application access or functionality. Examples of priority 1 issues include: faulty routers, server failure, or disk failure on a non-replicated disk. Priority 2 issues: Significant Impact: Priority 2 issues involve critical components that are degraded, or important functionality is not available. Examples include: moderate server faults where users may notice degraded system performance, failure to a replicated web server, or disk failure in a mirrored raid environment.. Priority 3 issues: Minor Impact: Priority 3 issues involve non-critical components that are inoperative, or are degraded. These are minor faults that the end-user may not noticed and cause little disruption in service. Examples of priority 3 issues include rebooting of a replicated router, restarting aborted processes, or memory short-runs. Priority 4 issues: No immediate impact. Priority 4 issues are generally non-outage situations involving requests for information. An example of priority 4 issues would be a request for the version of software on a server, or filling out a questionnaire.
Performance Category	4.0 Problem Resolution Rate
Performance Metric	The resolution rate measures the percentage of problems that are resolved within the established timeframes. Maximum response times are established to ensure all problems are resolved expeditiously.
Threshold Levels	Problem resolution rate: Priority 1 Critical: 95% Compliance with the following timeframes, no problem will exceed 12 hours. Essential - Premier: Less than 4 hours Priority 2 Major Impact: 95% Compliance with the following timeframes, no problem will exceed 24 hours. Essential: Less than 8 hours Enhanced: Less than 8 hours Premier: Less than 4 hours Priority 3 Moderate Impact: 95% Compliance with the following timeframes, no problem will exceed 4 days. Essential - Premier: Less than 2 days Priority 4 Minor Impact: 95% Compliance with the

	following timeframes, no problem will exceed 48 hours. Essential - Premier: Less than 8 hours Password Resets: 95% Compliance with the following timeframes, no problem will exceed 2 hours. Essential - Premier: Less than 30 minutes
Formula	Total number of problems resolved within the defined time frames divided by the total number of problems that have occurred. For example, 20 trouble tickets at priority 3 were received by the contractor help desk, 18 were resolved within the timeframes, 1 was resolved in 3 days, and 1 was resolved in 5 days. The formula would be 18/20 = .90. 90 percent is not in compliance, nor is the 1 trouble ticket that took 5 days to resolve.
Assumptions	The contractor's monitoring software should detect the vast majority of the problems that will affect an application's performance. The start of the problem resolutions begins when the monitoring software detects events that affect the application's performance. Another way of reporting a problem is through trouble tickets. Under NMCI the end-user will notify the NMCI help desk if there are problems with the application. If the NMCI help desk believe that the problem originates at the host environment, they will pass the trouble ticket to the contractor's help desk. The time that the contractor's help desk receives the trouble ticket from the NMCI help desk is when the time starts for problem resolution within the contractor's host environment. The contractor's help desk will categorize the problem and assign responsibilities for resolution appropriately. The contractor will be able to accept trouble tickets generated from the NMCI help desk. The contractor does not have to have the same software as NMCI, but they must have a process for receiving and responding to trouble tickets generated by the NMCI help desk. When the contractor's help desk provides feedback on a problem, they must provide a categorization of the problem, and the agreed upon timeframes for resolution. If the end-user does not agree with the categorization of the problem, the issue can be escalated to the CTR for resolution.
Contractor Responsibility	The contractor must have a process in place to monitor

	and document problems in the host environment. Documenting problems identified by the monitoring software is essential in trend analysis and long-term problem resolution. The contractor must also have a system in place to accurately categorize problems into their respective category. The contractor must have procedures in place to communicate responses and resolutions back to the NMCI help desk. In addition the contractor must provide feedback to the end-user detailing estimated resolution timeframes, based on problem severity
Customer Responsibility	The CTR must review the trouble tickets and monitoring logs to ensure that the appropriate categorization was assigned to the trouble ticket. Navy personnel or their associated contractors will assist in problem resolution with issues that may point to the application software as the cause of the problem.
Frequency	Monthly
Measurement Techniques	Response times are based on the hours of support and are calculated by subtracting the time the trouble ticket was received by the contractor's help desk to the time the trouble ticket was closed out, indicating that the problem was successfully resolved. Response times associated with problems identified by monitoring tools will start when resource thresholds are violated, or the tools indicate that application performance is degraded. Example (1) Hours of Support 24 X 7 A Priority 2 problem was reported to the NMCI help desk. NMCI staff determined that the problem was at the host environment. They passed the trouble ticket to the contractor's help desk. The contractor received the trouble ticket from NMCI at 16:55. The contractor responds at 17:05 Response time = 10 minutes The response time is calculated by subtracting the time the trouble ticket was received from NMCI from the time the contractor responded to the problem. 17:05 – 16:55 = 10 minutes Example (2): Hours of Support = 5 X 9 (08:00 – 17:00) Priority 2 problem reported in a monitoring toolat 16:55. Contractor Responds at 08:05 the next day.

	Response time is 10 minutes The response time is calculated by subtracting the time of threshold violation 16:55 from the end of the hours of support for that day 17:00, and then adding the difference between the start of the hours of support for the following day and the time the response was made. (17:00 – 16:55) + (08:05 - 08:00) = 5 + 5 = or 10 minutes. The CTR will review monitoring logs and trouble tickets received from the NMCI help desk, as well as those that may have been called directly into the contractor's help desk to determine resolution timeframes. In some cases developers will notice problems with the servers, and they should interface directly with the contractor help desk.
Reports	1. NMCI Trouble tickets 2. Contractor's trouble tickets 3. Monitoring tool reports
Person Responsible for Verification	The CTR is responsible for verification.
Escalation Procedures	The CTR must be contacted if the maximum time frames for problem resolution are exceeded. If there are disputes concerning the categorization of problems, the CTR will resolve the issue. It is important that all parties understand how to categorize the severity of the problems before application support begins.
Contractual Exceptions	Response times are only applicable during support hours.
Penalties/Rewards	Minor penalty: 5% of monthly rate • Threshold values exceed agreed upon rates. Major penalty: 20% monthly rate • Threshold values fall below 85% compliance for any of the timeframes. • Problem resolution is more than twice the agreed upon maximum response time.

Service Name	SLA 5.0: Request Management
Service Description	Request management measures the contractor's ability to respond to service requests from the government. The contractor must have a process in place to receive requests, perform requirements review to ensure they understand the request, execute the request, track execution status, , and report request completion.
Reason for Measuring	The government expects quality service. One type of service is request management, which measures the speed with which a contractor reacts to and completes a service request. Consistent time frames for implementing service requests, such as complex configuration changes are needed to accurately forecast completion times. Request metrics can be used in project scheduling, budgeting, and planning.
Time Frame	Derived by the selected hours of support. The default is 24 X 7.
Scope	Request services apply to requests that effect host environment hardware and software, and do not apply to application software. Examples of request services include: Platform design services, hardware configuration changes, large-scale software maintenance (e.g., upgrading to a new operating system), or software maintenance that involves coordination between client and server software releases (such as changing to a new version of a DBMS). Request services do not cover requests associated with problem resolution nor does it cover requests for normal software maintenance. Those areas are covered under separate SLAs. Level 1 High Application Impact: Examples of level 1 requests are changes that have a significant impact on the majority of end-users, , are difficult to reverse once they are applied, are highly complex such as designing platform solutions, or require a great deal of coordination. Level 2 Moderate Application Impact: Level 2 requests affect the application, but not the end-users. Examples of level 2 requests are modifications to peripheral hardware, adding additional agents to monitor resources, adding additional server resources, or installing shared services.

	Level 3 Minor Application Impact: Level 3 changes have little, if any, impact on the application itself. Examples are modifications to the infrastructure such as modifying the access control list in the firewall, requests for facility access, adding user identification/passwords for access to the server, and routine requests that do not fall anywhere else.

Performance Category	5.0 Response Time
Performance Metric	The metric measures the compliance with adhering to the time frames established for responding to requests.
Threshold Levels	Level 1 Major Application Impact: Essential - Premier: 15 Days to develop and propose a project plan. Resolution time frames will be negotiated between the government and the contractor. Level 2 Moderate Application Impact: Essential - Premier: 5 Days to develop implementation plan, 10 Days to complete request. Level 3 Minor Application Impact: Essential - Premier: 2 Days to complete request.
Formula	Calculate the time that the trouble ticket was initiated until the trouble ticket was closed out, indicating that the request was performed to the customer's satisfaction.
Assumptions	Funding for any requests that are not covered within the scope of the contract will be negotiated separately. The timeframes in this SLA will not be impacted by the time it takes to successfully negotiate for additional services. This includes the time it takes the contractor to develop an estimate of the costs associated with executing the request. The government and the contractor agree on the level of the request and the Change Review Board approves any proposed configuration changes. Level 1 request completion times will have to be negotiated separately. Estimated completion times will have to consider complexity, operational schedules, and coordination concerns. Both the government and the contractor will agree to the estimated project completion times.
Contractor Responsibility	The contractor must provide the documented policies and procedures for submitting changes and requests. The

	procedures will include the use of the contractor's help desk to record the initial request for service on a trouble ticket. Trouble tickets will be used to measure the time the request was submitted until the request was completed. The contractor must also provide a coordinator to manage the requests.
Customer Responsibility	The government will submit requests in compliance with the documented policies and procedures. The CTR will determine the request level. If the distinction is not clear, the CTR, contractor and program manager can negotiate a response time that is acceptable to all parties.
Frequency	Monthly
Measurement Techniques	Times are calculated by subtracting the time the trouble call is submitted until a project plan is delivered, and/or the request is completed. The total number of requests will be categorized into those that met the threshold levels and those that did not. The numbers will then be utilized in the formula to determine compliance.
Reports	1. Trouble tickets
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	5.1 Project Completion
Performance Metric	The metric used is a percentage of time that the actual project completion date deviated from the estimate in the project plan.
Threshold Levels	The thresholds apply to the timeframes established by SLA 5.0, or to the timeframes presented in the approved project plan. The following thresholds represent an acceptable percentage deviation from the promised completion date: Essential: 15 percent Enhanced: 15 percent Premier: 10 percent
Formula	The difference between the actual time to complete the request (AT) minus the estimated time to complete the request as outlined in the project plan (ET) divided by the estimated time. Formula = (AT – ET)/ET * 100 Actual time = 17 days Estimated time = 14 days

	Formula = (17-14)/14 * 100 = 21.43 percent
Assumptions	The government and the contractor agree on the project completion estimates before the contractor agrees to perform the request. Additional requirement or scheduling changes by the government will require a renegotiation of the estimated completion times. Level 1 tasks that can be performed in less than 10 days will default to level 2, and the thresholds for level 2 will apply. The time of request completion will be entered on the trouble ticket and the job will be closed out.
Contractor Responsibility	The contractor will provide an estimate of the time it will take to complete the request. The estimate will be part of the project or implementation plan.
Customer Responsibility	Review the estimated completion time to determine if the time frames meet operational commitments. Agree on time frames for completion before any work is actually performed. Allow the contractor adequate time to properly scope and research the request. What may appear to be a simple request may in fact be very complex.
Frequency	This SLA will apply to every request on a case-by-case basis. The CTR will apply any penalties at the end of the month in which thresholds were violated.
Measurement Techniques	The actual completion times for a level 1 request (taken from the trouble ticket) will be compared to the project completion estimate in the project plan. If the time actually completed exceeds the estimate, then the percentage of time difference needs to be computed.
Reports	1. Trouble tickets 2. Implementation plans: As they are developed
Person Responsible for Verification	The CTR will be responsible for verification.
Escalation Procedures	Any disputes will be resolved by the CTR. If there are still conflicts, the COR will make the final determination.
Contractual Exceptions	None
Penalties/Rewards	Minor penalty: 5% monthly rate • Threshold values exceed agreed upon rates.

	Major penalty: 15% monthly rate. • 5.0 Response Time Level 1 through level 3: compliance rate less than 85%. • 5.1 Project Completion Level 1: Project completion time exceeds 25% for Essential and Enhanced, and 20% for premium. • 5.1 Project Completion Level 2 and level 3: Time to complete the request exceeds 25% of the threshold.

Service Name	SLA 6.0: Security Management
Service Description	Security Management Services are those services required to protect the confidentiality, integrity and availability of the compute environment. The services include vulnerability assessments, intrusion detection, virus protection and compliance with DoD, and DoN policies and procedures.
Reason for Measuring	The Internet is an inherently untrustworthy medium. Any system that has connectivity to the Internet must have defensive systems, policies, and procedures in place to protect against attack. Many applications in the government contain information that is business sensitive. The sensitive but unclassified classification assigned to that information requires that the government take aggressive steps to ensure the confidentiality and integrity of the information. Information warfare or cyber-terrorism seeks to exploit security vulnerabilities to gather information, insert erroneous information, destroy information, and disable systems. A successful attack against a system or application can result in compromised information and hours or days of down time, depending upon the severity of the attack. Determining the extent of the damage can take days or weeks. An attacker may have penetrated the system months before; so corrupted files would be incorporated into the backup tapes. Without strong security measures it can be very difficult to determine when an attack occurred, and the extent of the damage.
Time Frame	Derived by the selected hours of support. The default is 24 X 7. Security monitoring is 24 X 7 regardless of the selected hours of support.
Scope	Security management includes the firewall, network and server hardware and software within the host environment, and does not apply to application software.

Performance Category	6.0 DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Certification
Performance Metric	The DITSCAP documentation outlined in DoD Instruction 5200.40 states that the environment and all applications residing in that environment must be certified. This metric measures compliancy with the DITSCAP program. The metric is a percentage expressed as the number of applications certified in accordance with the DITSCAP program divided by the total number of applications in the host environment.

Threshold Levels	The DITSCAP documentation includes a security risk assessment of the host environment (firewall, network, servers, and all supporting software) and each of the applications that reside in that environment. The thresholds are split between the host environment assessment and the individual application's risk assessments. The following thresholds apply to the certification of the host environment: Enhanced – Premier: 100 percent The following thresholds apply to the certification of applications within the host environment: Enhanced – Premier: 95 percent
Formula	The number of applications certified in accordance with the DITSCAP regulations divided by the total number of applications in the host environment.
Assumptions	The information in the DITSCAP documentation will be classified in accordance with the appropriate classification guide. The DITSCAP program refers to systems and not individual applications. However, the intent of the program is to gather enough information on the application to accurately determine the application's security risk. The DITSCAP documentation for the host environment will consist of the assessment of the security risks associated with the environment, and the appropriate documentation assessing the risk for each application. The contractor is responsible for the host environment assessment, and the government is responsible for the application specific documentation. At a minimum, the government activity will provide a type or system accreditation document approved by the developmental Designated Approving Authority (DAA) to be included in the contractor's host environment accreditation document. See NIST Special Pub 800-37, Guidelines for Security Certification and Accreditation of Federal Information Technology Systems for definitions. The government developmental (DAA) will evaluate the DITSCAP documentation, review the security risks, and determine if the system or application will be hosted in the contractor's host environment.

Contractor Responsibility	The contractor if responsible for certifying the host environment, as well as obtaining documentation from the government identifying the risks associated with the applications to be hosted in the host environment. The will be present the DITSCAP documentation to the appropriate government developmental DAA for review.
Customer Responsibility	Provide the contractor with the type or system accreditation documentation identifying security risks associated with the application. If a System Security Authorization Agreement (SSAA) already exists, provide the document to the contractor for incorporation into the contractor's accreditation documentation. If the customer needs assistance in documenting the appropriate risk information, the contractor can perform that function, however that task will be negotiated separately.
Frequency	This review will be conducted on a quarterly basis.
Measurement Techniques	The software configuration documentation will contain an inventory of all software in the host environment. The Information System Security Manager (ISSM) will spot check the configuration document against the SSAA to ensure that the proper information has been collected on the application. The ISSM will also have a listing of all applications that are hosted in the contractor's environment. Every application should have the appropriate DITSCAP documentation. The ISSM will check the periodicity of the host environment SSAA to ensure that it is renewed every three years.
Reports	1. A listing of all applications hosted with the contractor 2. The contractor's software configuration database. 3. The contractor's DITSCAP documentation that will include the host environment documentation as well as the documentation for every application.
Person Responsible for Verification	The appropriate government ISSM.

Performance Category	6.1 Adherence to Security Policies and Procedures
Performance Metric	The metric applied to security policies is based on spot checks performed by the government to validate that the contractor is abiding by DoD, DoN and contractor mandated security policies and procedures. The metric will be expressed as a percentage of spot checks showing adherence to policies divided by the total number of spot

	checks.
Threshold Levels	This performance category will evaluate how well the daily operations at the host environment abide by mandated security policies and procedures. Areas that will be evaluated include ensuring security changes can be traced back to approved change requests, users have the appropriate permission and access levels, passwords are the appropriate length, personnel with root access match the personnel approved to have root access, and physical security. DoD and DoN security policy states that successful intrusions must be reported. The incident report will be used as one of the spot checks for the quarter. If it is determined that the intrusion was a result of a failure to execute security procedures, then that spot check will count as a failed spot check. This review is separate from red team vulnerability assessments. The following thresholds apply to adherence to security policies and procedures: Enhanced – Premier: 95 percent
Formula	The number of spot checks indicating adherence with the mandated security policies and procedures divided by the total number of spot checks that were conducted.
Assumptions	The government will provide audit results to the contractor for comment. The contractor will take action to correct noted deficiencies. The audit results will be classified in accordance with the appropriate classification guide.
Contractor Responsibility	The government representative will have full access to all documentation, hardware, and software necessary to conduct the spot checks. The government expects full cooperation from the contractor.
Customer Responsibility	The government will provide the contractor with a checklist of the possible spot checks that will be performed. If discrepancies are discovered, the government will provide any necessary instructions or documentation to assist the contractor in correcting the problem. The appropriate ISSM will forward any modifications to the checklist, or any new DoD or DoN security guidance

	to the contractor.
Frequency	Quarterly
Measurement Techniques	The government representative will use an extensive checklist and personal knowledge to conduct the spot checks.
Reports	1. The security checklist. 2. The appropriate logs and reports to validate security procedures and policies are being adhered to 3. Configuration data to ensure security patches were installed.
Person Responsible for Verification	The appropriate government ISSM.

Performance Category	6.2 Access Revocation
Performance Metric	The metric to measure this category is the amount of time taken to remove an individual's access rights and privileges to the server.
Threshold Levels	As personnel rotate jobs, retire, or are terminated, their ability to access and/or authenticate to a server (password, PKI certificate) must be removed. This prevents hostile activity from a disgruntled worker, and it ensures that only authorized personnel have access to the server. Revoking access rights ensures that the authorized personnel are not held accountable for actions that may have been accomplished by someone no longer working with the server. This threshold applies to government personnel as well as the contractor's employees. The ISSM will notify the contractor when access rights for government employees need to be removed. Notification will be initiated through a trouble call to the server farm help desk. If contractor employees are terminated, transfer to another position that does not necessitate access to an application's server, or retire the ISSM will be notified within 8 working hours. The following thresholds apply to removing an individual's access rights: Enhanced – Premier: Less than 8 hours
Formula	For revocation of a government employees access rights, the time will be measured from the issuance of the trouble ticket to the completion time on the trouble ticket. If the revocation concerned a contractor employee, the time will

	be measured from the time the employee was removed from the project (as reported to the ISSM) until the time the employee's rights were removed. Log entries will detail the time the employee's rights were removed.
Assumptions	If a contractor employee is transferred to another position that does not need access to a server, the contractor will revoke that individual's access. The contractor will have to determine whether an internal employee needs access rights. In some cases, the contractor may want multiple employees to have access rights for redundancy purposes.
Contractor Responsibility	The contractor must notify the appropriate ISSM of contractor personnel terminated, retiring, or transferred off of the project. Notification must occur within 8 working hours after the individual has been terminated or reassigned.
Customer Responsibility	The customer is responsible for notifying the contractor of personnel that no longer need access to the server. Notification will be through a trouble ticket. The ISSM will notify the appropriate government personnel of contractor employee terminations or reassignments.
Frequency	Monthly
Measurement Techniques	The ISSM will use the trouble tickets, notification received from the contractor, and server logs to compute the formula.
Reports	1. Database of users and corresponding access rights. 2. Trouble tickets 3. Server logs
Person Responsible for Verification	The appropriate government ISSM.

Performance Category	6.3 Red Team Vulnerability Assessment
Performance Metric	The red team is a government security team that will evaluate the host environment for vulnerabilities. The metric used will be the success rate at preventing an attacker from affecting the integrity, confidentiality, or availability of data or systems hosted in the contractor's environment. The metric will be a percentage representing the amount of unsuccessful attempts to breach security in the area being assessed divided by the total attempts to breach security in the area assessed (for example, blocking denial of service attacks).
Threshold Levels	The red teams will test all aspects of the host environment security. They will evaluate a number of areas including,

	but not limited to: physical security, personnel security, firewall compliance, system penetration, planting (e.g., Trojan horse), data integrity, denial of service, virus protection, media security, communication monitoring, communication tampering, administrative security procedures, authorization violation, and authentication. Successful red team attacks against components that are in full compliance with DoD/DoN guidance and industry standards will not count against threshold figures. Threshold levels are as follows: Enhanced – Premier: 99.00 percent
Formula	The number of unsuccessful attacks divided by the number of total attacks. An attack is defined as an attempt to exploit a vulnerability by utilizing one form of attack. For example using a war dialer to determine the phone numbers of the modem bank constitutes one attack, even if 10,000 phone numbers were dialed. Denial of service attacks against one port constitutes one attack even if numerous messages were sent to that port.
Assumptions	The first red team assessment will be used as a training mechanism, and will incur no penalties for identified vulnerabilities. The red team will provide a brief to the contractor's management to explain the purpose of the assessment and to get their authorization to conduct the test. The red team will also provide a debrief explaining the results of the assessment. Government personnel will also be invited to the briefs. The results of the red team assessment will be classified in accordance with the appropriate classification guide. The red team assessment will have minimal impact on the applications residing in the host environment. If SLAs are affected as a result of the red team assessment, the contractor will not be penalized.
Contractor Responsibility	The contractor will provide full cooperation with the red team, including granting full access to the host environment (it is assumed that they will be escorted).
Customer Responsibility	The customer will provide the contractor with the vulnerability assessment results so appropriate action can be taken to correct or reduce the vulnerabilities identified.
Frequency	If a host environment has not received a red team

	assessment within 1 year, then the assessment should be done before the application becomes operational. Otherwise the periodicity is annual.
Measurement Techniques	The red team results will contain the information to apply to the formula. The red team will determine if an attack was successful.
Reports	1. Red Team vulnerability assessment
Person Responsible for Verification	The red team will perform the assessment, and the ISSM will verify the results against thresholds. If the ISSM does not have the appropriate security clearance to view the results of the assessment, then the verification will be conducted by a member of the Chief Information Officer's (CIO) staff with the appropriate clearance.

Performance Category	6.4 Correction of Red Team Identified Vulnerabilities
Performance Metric	The metric is the number of days to correct a deficiency or vulnerability identified in the red team attack.
Threshold Levels	The time to correct deficiencies should be prioritized by the criticality of the vulnerability, and the risk it presents to the application. Critical Vulnerability: The application is at risk from an attack that is commonly utilized (hackers have used the vulnerability to attack organizations more than 30 times). This categorization is subjective and will depend upon the red teams assessment of the vulnerability and the criticality of the application. The red team will make this determination. Moderate Risk: The vulnerability has been exploited in the past, but its risk is not high. The application would be affected, but not for any significant time (over 1 day). A denial of service attack would be an example of this type of risk. This is also a subjective assessment and the red team will make this determination. Non-critical Vulnerability: All other vulnerabilities identified by the red team. The time thresholds are as follows: Critical Vulnerability: Essential – Premier: 5 days Moderate Risk: Essential – Premier: 14 days Non-critical Vulnerability:

	Essential – Premier: 21 days Successful attacks against an application will have a direct impact on availability computations.
Formula	The time, expressed in days, from the red team debrief until the vulnerabilities are corrected, verified, and reported to the ISSM.
Assumptions	The red team will debrief the contractor on all identified security vulnerabilities. The red team will be available to answer questions from the contractor after the debrief.
Contractor Responsibility	Trouble tickets should be initiated to record actions necessary to correct vulnerabilities. The description on the trouble tickets does not have to detail specific vulnerabilities (e.g., tasks necessary to correct discrepancy #5). The contractor will correct the vulnerabilities and notify the ISSM when each is corrected.
Customer Responsibility	The ISSM will verify when the vulnerability has been corrected. The ISSM should be able to accomplish verification by physical inspection, working with the red team to replicate the attack, discussing the issue with the contractor staff, or talking to the red team personnel and describing the corrective action.
Frequency	Annually
Measurement Techniques	The time is measured from the day after the red team debrief until the CTR has verified that the vulnerability has been corrected. The trouble tickets will be used to measure completion times.
Reports	1. Red Team vulnerability assessment 2. Appropriate logs and reports necessary to verify that vulnerabilities were corrected. 3. Trouble tickets
Person Responsible for Verification	The appropriate government ISSM.

Performance Category	6.5 Incidence Reporting
Performance Metric	The period of time from detection of a security breach to the report of that incident. It is the contractor's responsibility to provide security for the application. The purpose of reporting an incident to the Fleet Information Warfare Center is to capture information and generate statistics concerning cyber-attacks on government assets and data. The information also helps to determine the extent of the attack or the resultant damage (e.g., worm attacks).
Threshold Levels	Incident definitions and categories are outlined in the CJCSM 6510.01 of 15 March 2002. The corresponding timeframes and method of reporting are outlined in table

	B-10 of that same document. Reports will be made to the Fleet Information Warfare Center (FIWC), and the ISSM assigned to the activity of the application supported. The CJCSM 6510.01 states the information required for the report. The ISSM is notified within 4 hours of the incident: Essential – Premier: 100%
Formula	The time expressed in minutes from the initial detection until a report is properly filed (in accordance with CJCSM 6510.01).
Assumptions	Taking action to mitigate the impact of an incident takes precedence over reporting criteria.
Contractor Responsibility	Upon detection of an incident, the contractor will make an initial report within the timelines outlined in CJCSM 6510.01. If all information is not available within the timeframes, submit a partial report, and follow up later when all of the information is known. The contractor will notify the appropriate ISSM of the incident as soon as possible (no more than 4 hours after the incident).
Customer Responsibility	The customer will provide the incident reporting documentation, and all points of contact for incident reporting. The customer will provide the contractor training on how to respond to incidents and fill out the appropriate forms. The customer will provide the contractor with recall numbers to notify the appropriate government personnel in the case of an incident.
Frequency	As an incident occurs. Each incident will be measured individually.
Measurement Techniques	Security logs from the firewall, network and servers will be reviewed to determine when an incident has occurred. The initial report will also indicate the time of discovery. If the security logs do not indicate an incident, the time on the report can be used. The ISSM will compare the time the contractor provided notice, to the time of incident discovery to determine the threshold for notifying the ISSM.
Reports	1. The appropriate security logs 2. Reports from monitoring tools 3. Reports from FIWC 4. The incident report generated by the contractor
Person Responsible for Verification	The appropriate government ISSM.

Performance Category	6.6 IAVA, NAVCIRT, and INFOCON Response
Performance Metric	The time measured in hours from when the government

	notifies the contractor of an Information Assurance Vulnerability Alert (IAVA), Naval Computer Incident Response Team (NAVCIRT) advisory or Information Condition (INFOCON) action, and when the action has been completed.
Threshold Levels	IAVAs, NAVCIRTs and INFOCON advisories are issued to prevent security incidents from occurring. These advisories identify newly discovered or recently exploited vulnerabilities and outline action to correct or mitigate those vulnerabilities. Each advisory gives a time frame for complying with and reporting the actions outlined in the advisory. In the case of INFOCON alerts, compliance may be required within the hour, but these are rare occurrences. The timeframes for complying and reporting compliance will determine the threshold timeframes. Reports will be made through the activity ISSM.
Formula	The time period from when the advisory was reported as a trouble call and the time that compliance was reported to the ISSM.
Assumptions	If any of the actions mandated by an advisory adversely affects the operation of the host environment, (e.g., interferes with monitoring agents, system settings, IDS agents) the ISSM will be notified, and a resolution will be determined.
Contractor Responsibility	The contractor is safeguarding government data. As such adherence to IAVAs, NAVCIRTS and INFOCON is required. The contractor will notify the appropriate ISSM when the actions outlined in the advisories have been completed.
Customer Responsibility	The ISSM will initiate a trouble call to the server help desk notifying the contractor of receipt of an IAVAs, NAVCIRTS and INFOCON. The ISSM will then deliver the alert to the contractor (fax, e-mail) as soon as they are received.
Frequency	Each advisory will be tracked individually.

Measurement Techniques	The ISSM will initiate a trouble call informing the contractor that they need to take action on an advisory. The ISSM will e-mail the advisory (a confirmation of receipt is required), or fax it to the contractor (a follow up phone call confirming receipt is required). The advisory will contain the time frame for compliance. That time period sets the threshold. The time from when the trouble ticket was submitted until the contractor reports compliance will be measured against the time requirement in the advisory to determine compliance.
Reports	1. IAVA, NAVCIRT or INFOCON messages 2. Trouble tickets
Person Responsible for Verification	The appropriate government ISSM.
Escalation Procedures	The activity DAA and associated ISSMs will be notified of vulnerability results. The CTR will be notified if any thresholds are violated. Any disputes will be resolved by the CTR. If there are still conflicts, the COR will make the final determination.
Contractual Exceptions	The initial red team attack will evaluate vulnerabilities and adherence to DoD and DoN policies and guidance. The results from the first vulnerability assessment will not count against this SLA. The first assessment will not only identify areas that need improvement, but will also clarify policy and procedural interpretation.
Penalties/Rewards	Minor penalty: 5% monthly rate • Any threshold values were exceeded. Major penalty: 15% monthly rate. • More than 4 minor penalties during the year. • 6.3 Success rate against red team less than 95% • 6.4 Correction of security vulnerabilities in the red team assessment or in an advisory exceeds 20% of thresholds. If time periods exceed 20% of threshold, there will be a 5% monthly rate penalty for every week until compliance.

Service Name	7.0 Software Maintenance
Service Description	Software maintenance involves installing new files, updates, or patches to the infrastructure, DBMS, and system software. For the purposes of this service level agreement, the terms patches, upgrades, and modifications are all considered maintenance actions, and the terms will mean the same. This SLA is concerned with the time it takes to realize that an upgrade to software in the host environment has been released until it is tested and finally installed in the production environment. This SLA does not cover the development of the maintenance software, nor does it cover the quality of the maintenance software. In most cases the software upgrade is from a third party vendor, and the quality of the software upgrade is a risk that the contractor must incur and manage. Software maintenance also has to be performed on the application, and its associated software. If the maintenance action requires root access to install the changes, then assistance will be required from the contractor, as only the contractor has full root control.
Reason for Measuring	Upgrades are generally released to correct problems with the software (bugs), update software to prevent new attacks, or to add/enhance functionality. The security of the application is dependent upon the speed at which the contractor installs security related updates. As a result it is important to place time frames on the contractor to ensure that security related patches and updates are installed as soon as possible. The contractor controls root access to the server. Application maintenance action requiring root access must be coordinated with the contractor. The threshold time frames are designed to give the contractor sufficient time to have staff available to assist with the installation of the application update. The government's maintenance

	personnel also have consistent response time frames that they can use to schedule their maintenance.
Time Frame	Derived by the selected hours of support. The default is 24 X 7.
Scope	Software maintenance covers all system, DBMS and infrastructure software. The software maintenance is only concerned with the software that resides in the host environment, and is not concerned with the client side of the software. Software maintenance concerns patches and upgrades to system and infrastructure software. The upgrades are not new releases of the software, but are supplements to existing installed versions. Upgrades to an existing version, (version 2.0) of application X, would be covered by this service level agreement, whereas installing a new version, (version3.0) would fall under the service level agreement for software refresh. Maintenance actions initiated by the government will not be constrained by this SLA. However, government initiated down time will not count against availability or contractor initiated maintenance time. Maintenance action to the application that does not require root access is not covered under this SLA. Tuning operating system software is not covered under this SLA. Tuning is considered a routine operation necessary to host an application.

Performance Category	7.0 Installation Time Frames
Performance Metric	The metric is the amount of time from release of a patch or update, until it is tested and installed.
Threshold Levels	System, DBMS, and infrastructure software installation priorities are as follows: Priority 1: Critical Security Related Patches. An example would be alerts covered under an IAVA or NAVCIRT. However, government generated alerts are covered under another SLA. This SLA is concerned with third party vendors, or the contractor, releasing patches in response to newly identified vulnerabilities. Priority 2: Routine Security Patches. Examples are virus or IDS signature updates.

	Priority 3: Upgrades correcting known errors: Examples are upgrades correcting functional problems, such as interfacing with new drivers. Priority 4: Routine upgrades or patches: Examples are upgrades adding new functionality. Thresholds are as follows: Priority 1 Maintenance Action: Essential – Priority: Within 8 hours from release from third party vendor. Priority 2 Maintenance Action: Essential – Priority: Submit to test lab within 1 day after release. Install within 3 days of release. Priority 3 Maintenance Action: Essential – Priority: Submit to test lab within 1 week after release. Submit the maintenance action to the configuration review board (CRB) at the first opportunity. Install within 1 week from CRB approval. Priority 4 Maintenance Action: Essential – Priority: Submit to test lab within 2 weeks of release. Submit the maintenance action to the configuration review board (CRB) at the first opportunity. Install within 1 week from CRB approval.
Formula	The time from the release of the patch or update to the time it is tested and installed.
Assumptions	Government personnel will notify the contractor of any priority 1 maintenance actions initiated from the government. Priority alerts from commercial sources will be the responsibility of the contractor. It is assumed that the contractor will subscribe to security alert services. If a third party's security patch is included in an IAVA, or NAVCIRT, the timeframes for installation will default to the government alert instead of this SLA. Due to the short timeframes involved with installing priority 1 maintenance actions, the CRB will be notified after the installation has been completed. Notification will be made through the government ISSM. Priority 2 maintenance actions are considered routine and part of daily business, and do not require the approval of

	the CRB. All maintenance actions must be properly documented. All maintenance actions will be annotated on the weekly schedule maintenance plan. Priority 3 and 4 maintenance actions will be performed during the maintenance window.
Contractor Responsibility	The contractor will develop procedures to ensure that the time frames are met. The contractor must annotate the release date of a patch or upgrade on the scheduled maintenance plan. All priority 3 and 4 maintenance actions must be presented and approved by the change review board. The contractor will notify the ISSM after any priority 1 patches are installed. Notification will be no later than the day following the installation.
Customer Responsibility	Notify the contractor of any government issued security alerts.
Frequency	Monthly
Measurement Techniques	The ISSM can check compliance with priority 1 maintenance actions by reviewing the trouble tickets and monitoring logs, and comparing those entries to the date the vendor released the update. The ISSM can check Internet history logs to determine if the contractor is downloading security patches on a daily basis. Software configuration documentation will list when those security patches were installed. The history logs will also ensure that the contractor is checking vendor's web sites, or monitoring security bulletins on a daily basis for new software patches or upgrades. The ISSM can check the software release dates on the scheduled weekly maintenance report, and compare those to actual release dates by calling the central design agency (CDA). The actual software release dates can be compared to the CRB notes to ensure that the maintenance action was presented to the CRB at the first opportunity. The CRB notes will contain approved maintenance action. The software configuration documentation will contain

	the date the software update was installed. The ISSM can check the dates to ensure the maintenance action was performed within 1 week of CRB approval.
Reports	1. Scheduled Maintenance Report 2. Server Logs 3. CRB Minutes 4. Software Configuration Documentation 5. Internet History Logs
Person Responsible for Verification	The appropriate ISSM

Performance Category	7.1 Root Access Assistance
Performance Metric	Only the contractor has root access to the operating system. As such, application developers needing access to files requiring root authority will have to coordinate with the contractor for access. This metric measures the time from the request for root access assistance until the application upgrade installation begins. This SLA affects application problem resolution because in some cases root access will be needed to restore corrupted or missing files.
Threshold Levels	Installation of application upgrades requiring root access is broken into three levels. Level 1: Installing Critical Application Upgrades: Examples include repairing security vulnerabilities, or significant functional errors. Level 2: Installing Serious Application Upgrades: Examples include repairing degraded functionality or performance. Level 3: Installing Routine Application Upgrades: Examples include adding new functionality. Thresholds are as follows: Level 1: Critical Upgrades Essential – Premier: Grant root access 4 hours after notification. Level 2: Serious Upgrades Essential – Enhanced: Grant root access 8 hours after notification Premier: Grant root access 4 hours after notification. Level 3: Routine Upgrades

	Essential – Premier: Grant root access within 3 working day after notification.
Formula	The time of the request for root access assistance minus the time that the application upgrade installation begins.
Assumptions	The government will perform the actual application upgrade installation. The contractor is only needed to grant root access to the government personnel. The CTR will track all government initiated maintenance actions to ensure that the maintenance down time is not charged against the contractor. The software configuration documentation will include not only the time frames for application upgrade installation, but also all pertinent information about the upgrade such as a detailed description, developer, purpose of the upgrade, and patch/version number.
Contractor Responsibility	Ensure that personnel are available and trained to grant root access during scheduled support hours. After hours personnel must be accessible by phone or pager to respond to after support hour level 1 root access requests. The contractor help desk will be used to generate a trouble ticket for root access requests. The help desk will determine the appropriate level. If there are disputes concerning level 1 requests, the contractor will grant the request and file a grievance through the CTR for resolution.
Customer Responsibility	The CTR will initiate contractor assistance through a trouble call to the contractor's help desk. The government maintenance personnel must inform the CTR if the maintenance action affected the application. If the application was impacted as a result of the maintenance action, that 'down time' will not count against availability SLAs.
Frequency	Monthly
Measurement Techniques	The CTR will review the trouble ticket to determine the time between the request and the time the contractor granted root access to the server. The trouble tickets will be grouped into the three levels and the appropriate thresholds will be applied. The CTR can also review the maintenance records and configuration documentation to the times that the software was installed.
Reports	1. Trouble Tickets

	2. Software Configuration Documentation 3. Maintenance Records
Person Responsible for Verification	The CTR is responsible for verification.
Escalation Procedures	The CTR will attempt to resolve all disputes concerning the maintenance priorities or request levels. Disputes that cannot be resolved will be presented to the COR.
Contractual Exceptions	Maintenance downtime associated with application upgrades will not count against the contractor's availability or maintenance SLA thresholds.
Penalties/Rewards	Minor Penalty: No monetary penalty • Any threshold values were exceeded. Major Penalty: 25% of monthly rate. • More than 3 minor penalties in any maintenance category in one year. • Any of the priority 1-4 response thresholds for upgrades were exceeded by more than 50%. • If any of the level 1-3 response thresholds for root access were exceeded by more than 50%.

Service Name	SLA 8: Maintenance Schedules
Service Description	Maintenance in this SLA involves hardware and software maintenance. Hardware maintenance can involve changing routers, installing memory, or repartitioning drives. Software maintenance involves installing new files, updates, or patches to the infrastructure, DBMS, and system software. This service level agreement outlines the day and the times that will be used to perform maintenance that affects the application. The SLA also specifies the amount of time that the application is affected as a result of the maintenance actions throughout the month.
Reason for Measuring	Fixed maintenance windows set a level of user expectation. Users should not expect full access to an application during scheduled maintenance windows. Maintenance down time has direct business repercussions. When an application is not functioning, users cannot perform their jobs, schedules are affected, morale declines, and opportunities are lost. Specifying maintenance windows, and the total amount of maintenance down time allows an organization to take the application down time into consideration. Activities can be planned around the scheduled maintenance down time.
Time Frame	Derived by the selected hours of support. The default is 24 X 7.
Scope	Any hardware or software maintenance actions within the host environment (including the firewall) that affect the application will apply to this SLA. Maintenance to the application itself will not be covered under this SLA.

Performance Category	8.0 Maintenance Window
Performance Metric	This is the scheduled time period in which maintenance actions can occur.
Threshold Levels	The following thresholds apply: Essential: Sunday 0800-1200 Enhanced: Sunday 0800-1200 Premier: No scheduled downtime Any maintenance action performed outside of the maintenance window will count as application down time and will be used in the availability computations.

	Any deviations from the maintenance window will have to be approved by the application program manager. The CTR must be informed of any approved maintenance activity outside of the maintenance window.
Formula	None
Assumptions	Installation of security signatures on the IDS, anti-spam and anti-virus software will not require downtime.
Contractor Responsibility	All maintenance action initiated by the contractor will be performed within the maintenance window. Notify the CTR of scheduled maintenance action during the week.
Customer Responsibility	Inform users of the application that there may be difficulties in accessing the application during scheduled maintenance windows.
Frequency	Monthly
Measurement Techniques	The CTR will review the weekly maintenance schedule from the contractor. The maintenance should all be scheduled within the maintenance window. The CTR will review monitoring logs to ensure that the application was only "down" for maintenance time within the scheduled time frames. The CTR must be informed of any negotiated deviations from the maintenance window. Application down time not within the scheduled maintenance window will count against the availability SLA.
Reports	1. Maintenance schedule 2. Trouble tickets 3. Monitoring logs
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	8.1 Maintenance Hours
Performance Metric	This is the total scheduled maintenance time for the month.
Threshold Levels	The following thresholds apply: Essential: 4 hours Enhanced: 4 hours Premier: No scheduled downtime
Formula	Add the maintenance time during which the application was affected.
Assumptions	The change management board must approve all software maintenance actions, with the exception of emergency security updates. All maintenance action is tested before installation. In the case of emergency security installation, the application is tested after the installation. Tests will be conducted in accordance with the approved test plan.

	Any system or infrastructure down time outside of the scheduled maintenance time will be considered down time and will count against availability service level agreements. For example if the scheduled maintenance down time is 4 hours, and 5 hours were actually used to perform maintenance during the month, then 1 hour will be considered down time in the availability computations.
Contractor Responsibility	Notify the CTR of maintenance actions that will be scheduled during the week.
Customer Responsibility	The customer is responsible for notifying end-users if their access to the application will be affected by scheduled maintenance.
Frequency	Monthly
Measurement Techniques	The CTR will verify the scheduled maintenance down time against the system monitoring logs. The CTR will then calculate total maintenance time by adding the maintenance down time during the month.
Reports	1. Maintenance schedule 2. Monitoring logs
Person Responsible for Verification	The CTR is responsible for verification.
Escalation Procedures	The CTR will be notified of any deviations from the maintenance windows or schedules.
Contractual Exceptions	Scheduled maintenance initiated by the government will not be applied to this SLA.
Penalties/Rewards	Maintenance action outside of the schedule maintenance window, or maintenance down time exceeding thresholds will be considered down time for availability computations. Availability penalties will apply.

Service Name	9.0 Migration Services
Service Description	Migration services are those services required to move, install, and operate an application in the contractor's Application Hosting environment.
Reason for Measuring	Transition services are measured to ensure that the project is completed on time, and that the application's performance does not suffer as a result of being hosted in the contractor host environment.
Time Frame	This SLA covers the time period from contract award until the application is installed in the production environment, can be accessed by its intended end-users, and is fully operational. The completion time will be determined when the government validates that all migration requirements have been satisfied.
Scope	Migration in the context of hosting applications is the process by which an application is transferred from one platform to another. The specific tasks that need to be performed during the migration phase and the deliverables are specified in the statement of work (SOW). The scope covers all activities necessary to migrate the application to the contractor host facility, including application audits, designing activities, performing requisite testing (outlined in the migration plan), placing the application into the production environment, establishing connectivity, and operating the application at full functionality.
Performance Category	9.0 Implementation, Integration, and Test Service (IIT) Service Window.
Performance Metric	The metric establishes the amount of time to perform all actions required to migrate an application to the contractor's host environment.
Threshold Levels	The threshold levels are as follows: Essential Services: 3 months Enhanced Services: 3 months Premier Services: 3 months
Formula	The time is measured from the date the contract is awarded and concludes at documented acceptance of migration services.
Assumptions	Actions relating to estimating migration costs will not be included in the migration time. For example audits must be conducted on the application to properly scope a bid. The time necessary to conduct a preliminary audit will not

	count as migration time. Once the contract is awarded any subsequent audits will count as migration time.
Contractor Responsibility	The contractor must coordinate with the government for functional testing and access to the application. The contractor must understand and operate within the government's operational constraints.
Customer Responsibility	After the contract has been signed, the contractor must have access to the application and current hosting facilities to perform a full audit, and to package the application. The government may have to negotiate with third parties to obtain access permission.
Frequency	The frequency spans the time from contract award until the government documents acceptance of the migration action.
Measurement Techniques	The date that the government has documented acceptance of migration services is subtracted from the date the contract was awarded.
Reports	1. Hosting contract: It will determine threshold start times. 2. Migration plan: The government will document acceptance of migration services. This document will be incorporated into the migration plan for official acceptance.
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	9.1 Application Performance
Performance Metric	The metric used to test application performance will be an industry standard benchmark test. Areas measured will include areas such as input-output times, memory paging, bandwidth utilization, and processing speeds.
Threshold Levels	Threshold levels are based on a comparison of benchmark tests run in the previous host environment with identical tests run on the application in the contractor's host environment. The following thresholds apply: Essential – Premier: Identical or greater performance in all areas of the benchmark tests.
Formula	This will be a direct comparison of the benchmark tests in the two environments. The tests in the new environment should be equal to or exceed the results obtained in the previous host environment.
Assumptions	The government and the contractor will determine the benchmark tests to execute to test the performance of the application.
Contractor Responsibility	If the government has not determined which benchmark

	tests to utilize, the contractor will recommend industry standard benchmark tests to the government. Execute the benchmark tests on the application in both host environments and provide results to the CTR.
Customer Responsibility	The contractor must have full access (root) to the application and associated servers in the previous host environment in order to run the benchmark tests. The government is responsible for obtaining the cooperation of the staff in the previous host environment. The government will monitor the testing to understand any differences in how the benchmark test was applied. In some cases the differences in the tests occur as a result of configuration differences in the host environments. The government representative will ensure the results accurately measure the application's performance.
Frequency	This measurement is from the time that the contract is awarded until the government documents that all migration requirements have been met.
Measurement Techniques	The government representative will compare the application benchmark tests in both environments to ensure that the application's performance equals or is better in the contractor host environment.
Reports	1. Benchmark test results
Person Responsible for Verification	The CTR is responsible for verification. Verification in this case may require the assistance of the application developers to ensure the tests are run correctly.
Escalation Procedures	The contractor will notify the CTR if the migration cannot be accomplished within time frame thresholds. Designated government representative will approve results of the benchmark tests. COR will resolve all conflicts.
Contractual Exceptions	None
Penalties/Rewards	Minor penalty: 5% monthly rate • Any threshold values were exceeded. Major: 15% monthly rate • Migration transition times exceed 50% of the threshold. • Application benchmark tests in the new host environment do not meet or exceed the benchmark tests in the prior host environment. If there are application performance issues, the application will not be placed in operation until the problems are resolved.

Service Name	SLA 10 Backups
Service Description	Backups refer to the process of copying data, files, disks, or the entire application to tape. There are two general types of backups. A full backup contains all of the data in a file system. An incremental backup contains only those files that have changed since the last backup. This service level agreement will measure the accuracy of the backup, adherence to the back up schedule, accuracy of tape labeling, accuracy of tape library, and restoration timeframes.
Reason for Measuring	Computers are not 100 percent reliable, disk drives can fail, files and data can be corrupted, and disasters can destroy the entire system. If the information stored in the file system has any value, it must be backed up. Backups act as a form of redundancy, and are designed to protect the integrity of a system's data. If a disk drive crashes, the information on the backup tapes can be used to restore the system. Restoration speed, tapes accuracy, and the accuracy of the tape library affect the MTTR, which influences overall availability of the application. There may also legal requirements for the retention of financial data, audit logs, or other data required for possible investigations or audits.
Time Frame	The time frames is 24 X 7.
Scope	Backups refer to application software, system software, DBMS, database files, and system and monitoring logs hosted in the contractor's host environment. There are numerous DoD and DoN policies and directives concerning backups, such as on-site storage requirements, and protecting the security of the data on the tape. Adherence to those policies will be covered under the security SLA.
Performance Category	10.0 Backup Schedule
Performance Metric	The metric will measure the contractor's adherence to the backup schedule. The metric will be expressed as a percentage of backups performed within the schedule divided by the total number of backups that should have been performed. Adherence to the schedule is vital in protecting the data in the file systems. If an incident occurs where the files are destroyed, any data received, modified, or deleted from

	the time between the incident and the last backup is lost. This may have serious repercussions for mission critical, data intensive systems. If the schedule is not followed, the risk of loosing business essential data increases.
Threshold Levels	The normal backup schedule is where incremental backups are performed daily 6 times a week and a full backup is performed on Saturday or Sunday. Additionally a full monthly and end of year backup are performed. Once the backup tapes are created they must be stored for a period of time before they can be reused. It is possible for a file to be corrupted and not noticed for weeks or months because the file is rarely accessed. As a result, it is prudent to keep copies of the file systems for a reasonable period of time. The following is a recommended backup schedule with storage days: • Daily incremental backups must be stored for 8 days • Weekly full backups must be stored for 2 months • Monthly full backups must be stored for 12 months • Annual full backups must be stored for 5 years. The thresholds for conforming to the backup schedule are as follows: Enhanced – Premier: 99% The thresholds for conforming to the backup storage requirements are as follows: Enhanced – Premier: 99%
Formula	The number of backups performed within the backup schedule divided by the total number of scheduled backups. The number of backups stored within the storage requirements divided by the total number of stored tapes.
Assumptions	The contractor will be responsible for providing the tape media. The media can be reused, but after a period of time, the media degrades and must be replaced. The contractor is responsible for replacing the media.
Contractor Responsibility	Brief the application program manager on the backup schedules and procedures that will be used to backup the application.
Customer Responsibility	Cooperate with the contractor in developing the backup schedule and associated backup procedures for the application.
Frequency	Monthly
Measurement Techniques	The government auditor must perform spot checks to ensure the backups were conducted within the scheduled

	time frames, and that they are stored for the appropriate amount of time. The auditor will check the system logs and monitoring logs to determine when the backups were actually performed. The auditor will have to physically check the tape storage areas to ensure tapes are being stored for the appropriate amount of time. The tapes must be labeled with the date of the backup, so determining the storage time is simply a matter of ensuring all of the tapes for the required storage period are present. For example, when checking the daily tapes, there should be 7 days of backups available (1 day is a weekly update).
Reports	1. Monitoring logs 2. System logs 3. Backup schedule
Person Responsible for Verification	The CTR will be responsible for verification.

Performance Category	10.1 Tape Backup Accuracy
Performance Metric	This category measures the accuracy of the tape backup. If the system is not backed up correctly, then the system's data is not protected, and data critical to the organization could be lost. Tapes have a shelf life of approximately 3 years. After 3 years the files on the tape must be transferred to new medium. The accuracy of the file transfer from the old medium to the new medium will be included in this category. The measurement will be the percentage of files that were backed up correctly divided by the number of files that were spot-checked.
Threshold Levels	Backup accuracy thresholds are as follows: Essential: 99.5% Enhanced: 99.5% Premier: 99.7%
Formula	The number of files that were accurately backed up divided by the total number of files sampled.
Assumptions	Restoration should be performed on a test platform.
Contractor Responsibility	The contractor must implement backup software that verifies backed up files by reading the files after they are written to the tape. The contractor will assist the government representative with loading the tapes to conduct the spot checks.
Customer Responsibility	Coordinate with the contractor for performing the spot checks. Access to a test server will be required.
Frequency	Quarterly

Measurement Techniques	The proof that the files were correctly backed up is to read and/or restore the contents of the tape. A representative sample of tapes will be evaluated. Random files will be accessed to determine if they can be read. Other files will be restored. Sample files will be evaluated from each tape.
Reports	1. Tape library
Person Responsible for Verification	The CTR will be responsible for verification.

Performance Category	10.2 Tape Documentation Accuracy
Performance Metric	Tape documentation refers to the labeling on each tape, and the tape library documentation. It is essential that each tape be clearly and accurately labeled. The tape labels will have detailed information to uniquely identify their contents. Information such as date and time of the backup along with the format of the files will also be included. The tape library records at a minimum, the files stored on each uniquely numbered tape as well as the dates the files were backed up. The metric used will be a percentage of tapes accurately labeled and recorded in the tape library. If any of the files on the tape do not match the documentation of either the tape label or the tape library, then the tape documentation is considered incorrect. Tape documentation is essential in rapidly restoring files.
Threshold Levels	The following are the thresholds for backup documentation. Essential: 97% Enhanced: 97% Premier: 98%
Formula	The formula is the number of tapes accurately labeled and recorded in the tape library divided by the total number of tapes spot checked.
Assumptions	The documentation requirements in this SLA also pertain to backup media other than tapes.
Contractor Responsibility	Provide the necessary tape library documentation to perform the spot check. Assist the government representative with loading the tapes to conduct the spot check.
Customer Responsibility	Coordinate the spot check with the contractor. Allow enough time for the contractor to have the equipment and staff on hand to assist with the spot check.

Frequency	Quarterly
Measurement Techniques	The tapes will be loaded onto a platform for read access. The files contained in the tapes that are spot-checked will be evaluated against the tape label and the tape library.
Reports	1. Tape labels 2. Tape library
Person Responsible for Verification	The CTR will be responsible for verification.

Performance Category	10.3 Restoration Time Frames
Performance Metric	Restoration refers to the task of retrieving a file from a backup tape and installing it on a system. The first step is to determine which tape has the version of the file needed. The individual file then has to be found and copied to the system server. The backup copy of the file then replaces the missing or corrupted file on the server. This section refers specifically to restoring application related files. Restoration time for system software will be included in the overall timeframes for system availability or problem resolution. The files being restored are part of the application; as government personnel may require root access from the contractor. The performance metric is the time from the request to restore a fileuntil the file is installed and operational. The request will be placed with the contractor's help desk.
Threshold Levels	The restoration time thresholds will depend upon the severity of the problem necessitating the restore action. Priority 1 issues: Mission Critical Impact: Priority 1 issues involves loss of application access or functionality. Priority 2 issues: Significant Impact: Priority 2 issues involve degraded application functionality. Priority 3 issues: Minor Impact: Priority 3 issues involve minor faults that the end-user may not noticed and cause little disruption in service. Priority 3 issues also involve restoration of files for inspection or audit purposes. File restoration thresholds are as follows: Priority 1 Critical: 95% Compliance with the following time frames, no problem will exceed 12 hours. Essential: Less than 4 hours Enhanced: Less than 4 hours Premier: Less than 4 hours

	Priority 2 Major Impact: 95% Compliance with the following timeframes, no problem will exceed 24 hours. Essential: Less than 8 hours Enhanced: Less than 8 hours Premier: Less than 4 hours Priority 3 Moderate Impact: 95% Compliance with the following timeframes, no problem will exceed 4 days. Essential - Premier: Less than 2 days
Formula	The number of restoration procedures performed within stated thresholds divided by the total number of restoration procedures performed.
Assumptions	When a problem occurs, the NMCI help desk will field the trouble call. The trouble ticket will be passed to the contractor's help desk. If the problem points to the application itself, the government personnel will trouble shoot the application. If a file needs to be restored, the government personnel will place a trouble call to the contractor's help desk to start the restoration trouble ticket. The restoration times associated with problems with DBMS, infrastructure, or system software will count against availability calculations, and not this SLA.
Contractor Responsibility	Cooperate with the government personnel that are restoring the application files. If root access is required, that SLA will apply. The contractor's help desk will determine the priority level of the restoration request. The level of the request will be annotated on the trouble ticket. If there are disputes covering the priority of the request, grant the request and file a grievance through the CTR for resolution.
Customer Responsibility	The government will request file restoration using the contractor's help desk. The government will work with the contractor to train the help desk personnel determine the appropriate priority levels for requests.
Frequency	Monthly
Measurement Techniques	Review the trouble tickets for restoration services and determine whether any of the requests did not meet the designated time frames. Check restore times against server and monitoring logs, if designated time frames were violated; apply the formula to determine compliance with the thresholds.

Reports	1. Trouble tickets 2. Server logs 3. Monitoring logs
Person Responsible for Verification	The CTR is responsible for verification.
Escalation Procedures	The CTR will be notified of threshold violations. If there is disagreement concerning the categorization of priorities, the CTR will work with both the contractor and the CTR to resolve the issues. If the problems persist, the issue will be referred to the COR.
Contractual Exceptions	None
Penalties/Rewards	Minor penalty: 5% monthly rate • Any threshold values were exceeded. Major penalty: 20 % monthly rate • Three minor penalties within the year • 10.0 Backup schedule compliance in each service level (essential – Premier) is below 90% • 10.1 Backup Accuracy is below 95% in each service level • 10.2 Backup documentation accuracy in each service level is below 90% • 10.3 Restoration services exceed maximum response times for the priority assigned to the service.

Service Name	SLA 11 Batch Services
Service Description	Batch processing used to refer to the processing of a batch of punch cards. Today the term is used more to describe the sequential processing of data. Typically once a batch job begins, it continues until it is done or until an error occurs. The next sequential program is then run, until all programs have executed fully. Many financial programs contain batch processing, especially during reconciliation processes.
Reason for Measuring	Batch jobs require additional oversight because they must be run in sequence, and they usually must be run within specified time windows. When batch jobs are running, there is no user input into the program. As a result it is important that batch jobs are run efficiently, because users are locked from the program while the batch jobs are processing. Additionally, if any errors occur while processing a batch job, it must be run again, and any information processed must be either backed out, or over written.
Time Frame	The time frames is 24 X 7.
Scope	Batch jobs will be identified to the contractor during the migration audit. The contractor is responsible for maintaining a batch job schedule, which lists the batch job, and the time frames allotted for processing. This service level agreement refers to the batch jobs contained on the batch schedule. Maintaining a batch schedule is a systems administrator function, even though it directly supports an application, or its associated databases. As such, it is the responsibility of the contractor to run the batch jobs.

Performance Category	11.0 Batch Accuracy
Performance Metric	The batch job should execute as desired. If errors occur in the process, then the process should be run again. The contractor is responsible for monitoring batch program execution. The performance metric is a percentage of the programs executed within specifications divided by the total number of programs executed. Each sequential program is distinct. If the entire batch contains 15 sequential programs, then each program will be counted individually.
Threshold Levels	The thresholds for batch processing accuracy is as follows: Essential: N/A Enhanced: 99.5% Premier: 99.7%

Formula	The batch programs executed within specifications divided by the total number of programs executed.
Assumptions	The contractor must perform, or assist the government in batch program restarts. Detailed execution procedures will be developed for each batch job. If problems with the batch job persist, the contractor will notify the designated government personnel.
Contractor Responsibility	Ensure the batch job schedule is accurate, and the staff is properly trained to execute the batch programs.
Customer Responsibility	Ensure that the batch job schedule contains all of the batch jobs that pertain to an application. Provide the contractor all pertinent information to execute and monitor the batch jobs. This includes providing test scripts or a description of the expected output to ensure the program is executing to specifications.
Frequency	Monthly
Measurement Techniques	The CTR will review the batch processing monitoring reports and evaluate trouble tickets that may pertain to the batch jobs.
Reports	1. Trouble tickets 2. Monitoring logs 3. Server logs 4. Batch job schedule
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	11.1 Batch Job Completion
Performance Metric	Many batch jobs must be completed within a specific time window. The metric will be presented as the percentage of batch jobs executed successfully within the scheduled time frames. Recommended time frames are as follows: All daily, weekly and monthly batch runs must be completed by 0700 AM of the following business day. If a batch job is not completed by the deadline, the contractor and government must determine if the batch job should still be run, or if it should be terminated.
Threshold Levels	The thresholds for batch job completion are as follows: Essential: N/A Enhanced: 95% Premier: 95%
Formula	The formula will be the number of batch jobs executed within the scheduled time frames divided by the total number of batch jobs scheduled to be executed.
Assumptions	Government requests for batch job execution for jobs not listed on the schedule will not count against this SLA.

	The recommended time frames for batch processing will be modified to suit the needs of each application.
Contractor Responsibility	Notify the government representative if a batch job cannot be completed within the scheduled time frame.
Customer Responsibility	Work with the contractor to determine a course of action if a batch job is not processed by the deadline.
Frequency	Monthly
Measurement Techniques	Review the batch job schedule and the batch job monitoring report to determine any processing outside of the scheduled time frames. Divided the number of batch jobs completed within the time frames by the total number of scheduled batch runs.
Reports	1. Monitoring logs 2. Server logs 3. Batch job schedule
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	11.2 Batch Job Requests
Performance Metric	This category is concerned with the addition, deletion, modification, or stopping of a batch job. The batch job schedule may need to be modified for a number of reasons, including seasonal requirements, new regulations, changing business processes, new requirements, or errors were found in the program.
Threshold Levels	Response times for request to add to, delete from or modify the batch job schedule are contingent upon the impact that the batch job has to the organization's business process. Priority 1 issues: Mission Critical Impact: Priority 1 issues involves a critical impact to business processes. Priority 2 issues: Significant Impact: Priority 2 issues have a noticeable impact on business processes. Priority 3 issues: Minor Impact: Priority 3 issues are routine adjustments to the batch job schedule. Stop Action: There are instances where the batch jobs should not be run as scheduled. The government must give the contractor proper notification before the contractor can stop the batch job. Request response thresholds are as follows: Priority 1 Critical: 95% Compliance with the following

	timeframes, no request will exceed 12 hours. Essential: N/A Enhanced: Less than 4 hours Premier: Less than 4 hours Priority 2 Significant Impact: 95% Compliance with the following timeframes, no problem will exceed 24 hours. Essential: N/A Enhanced: Less than 8 hours Premier: Less than 8 hours Priority 3 Moderate Impact: 95% Compliance with the following timeframes, no problem will exceed 5 days. Essential – Premier: Less than 3 days Stop Action: Essential – Premier: The batch process will not be run if notification is given 1 hour before the scheduled run.
Formula	The number of requests that were satisfied within the time frames divided by the total number of requests.
Assumptions	Any requests to modify the batch jobs will have to be requested through the contractor's help desk.
Contractor Responsibility	Work with the program manager in determining criteria for categorizing the criticality of batch job requests.
Customer Responsibility	Give the contractor as much time as possible to make the modifications to the batch schedule. If adding or modifying batch jobs, ensure there are government personnel available to assist the contractor.
Frequency	Monthly
Measurement Techniques	The CTR will review the trouble tickets for requests and verify performance against the batch job monitoring reports.
Reports	1. Trouble tickets 2. Monitoring logs 3. Server logs 4. Batch job schedule
Person Responsible for Verification	The CTR is responsible for verification.
Escalation Procedures	The CTR will be notified of any threshold violations. The CTR will attempt to resolve all disputes. Disputes that cannot be resolved will be presented to the COR.
Contractual Exceptions	None

Penalties/Rewards	Minor penalty: 5% monthly rate • Any threshold values were exceeded. Major penalty: 20 % monthly rate • Three minor penalties within the year • 11.2 If any of the maximum time frames designated in the batch job request section were exceeded.

Service Name	SLA 12.0 Technology Refresh Rates
Service Description	Technology is changing at a rapid pace. To take advantage of new innovations, technology must be updated. This SLA specifies the time frames for technology refresh rates. Technology refresh requires coordination between the government and the contractor. The coordinator cannot upgrade to a new version of system software or hardware without ensuring that the application is not affected. Conversely the government must ensure that if the application developers are designing new functionality that requires an upgraded hardware or a new version of software that the contractor is willing and able to support the upgrade.
Reason for Measuring	Technology needs to be updated on a consistent basis, not only to take advantage of the benefits offered by that technology, but for interoperability purposes as well. Technology refresh also allows software developers the opportunity to take advantage of the most recent scientific advancements.
Time Frame	Quarterly
Scope	Technology refresh applies to all hardware and software in the contractor's host environment that supports the application, including firewalls.

Performance Category	12.0 Software Refresh
Performance Metric	The contractor is responsible for the planning, installation, and testing of system and infrastructure software upgrades. New software will not be installed upon release. The contractor must have time to test the new version, and develop an installation plan if the upgrade is extensive. However, the time from release to installation should be quick enough to allow the government to take advantage of any benefits, and to ensure interoperability. This SLA is concerned with the installation timeframes for new versions of software. Patches or upgrades to existing versions are covered under another SLA. The metric used will be the time from the release of the new software version until it is installed in an operational environment.
Threshold Levels	The following are the thresholds for software refresh: Essential: 18 months Enhanced: 12 months Premier: 6 months

	No system or infrastructure software will be more than 2 releases behind the most current software release.
Formula	None
Assumptions	Some legacy application software have dependencies that do not allow for system software upgrades. In the case of hard coded dependencies, only non-dependent software would be upgraded.
Contractor Responsibility	Notify the configuration review board of any software upgrades. This requires that the contractor keep abreast of latest changes in technology. It also requires that the contractor determine how the new changes will affect the hosted application. This will require testing and coordination with the government developers.
Customer Responsibility	Cooperate with the contractor in any functional tests required to test a new software release. The government developers should also be aware of and take advantage of the latest software releases.
Frequency	Quarterly
Measurement Techniques	The CTR will verify software refresh rates by reviewing recommendations from the vendor, minutes from the change review board, scheduled maintenance reports, configuration documentation, and spot-checking the latest releases with the applicable vendors.
Reports	1. Minutes from the Change Review Board 2. Scheduled maintenance reports 3. Configuration documentation 4. Software refresh recommendations from contractor
Person Responsible for Verification	The CTR is responsible for verification.
Escalation Procedures	The COR will be notified if there are any disagreements on interpretation.
Contractual Exceptions	None
Penalties/Rewards	Minor penalty: 5% monthly rate • Any threshold values were exceeded. Major penalty: 25 % monthly rate • Two minor penalties within the year

Service Name	SLA 13.0 Administration
Service Description	Administration is a general category that is concerned with ensuring documentation is up to date, accurate and is delivered in a timely manner. It also addresses attendance at required meetings and adhering to contractual procedures. The delivery of reports address the time frame that the various report deliverables must be delivered to the designated government representatives.
Reason for Measuring	Since many of the reports produced by the contactor are used to provide oversight of the contractor's performance, it is important that the reports are accurate and timely. Some reports are also used to perform quality control. If the information contained in those reports is delayed, potential corrective actions will also be delayed. Everyone's time is valuable. If a contractor is needed at a meeting, such as the configuration review board, it is important that a representative, with the appropriate power making authority attend, not only to represent the interests of the contractor, but also to ensure that the scheduled business can proceed.
Time Frame	The time frame is 24 X 7.
Scope	Delivery of Reports includes all the reports defined and agreed upon in the deliverables documentation. In addition to the reports defined in the deliverables document the contractor must also provide SLA compliance reports and associated reports that provide background, detailed information, or the raw information that may have been consolidated for the SLA reports. Delivery time frames are outlined in the statement of work or the corresponding deliverables section of the contract. Scheduled meetings refer to planned meetings that occur on a frequent basis, such as the configuration review board. It does not include short notice meetings that were not on the agreed upon meeting schedule. License management covers all software that is utilized in the contractor's host environment, including the application itself. Licenses for GOTS applications are not in the scope of this SLA. Change management procedures covers changes made to

	any software or hardware in the contractor's host environment, including the application. The contractor and the government will promulgate the change management procedures in a change management document that will be mutually agreed upon. This plan will discuss how the change review board will function, requirements for documenting the change, and testing requirements.

Performance Category	13.0 Delivery Schedule
Performance Metric	The contracted delivery time frames for the document deliverables will be evaluated against the actual delivery time.
Threshold Levels	The thresholds are as follows: Essential – Premier: Reports are due within one business day of their due date.
Formula	None
Assumptions	Government requests for reports that are not specified in the contract will go through the CTR for contract scope determination. If the contractor agrees, the request will be categorized as a priority 4 problem resolution and will require a trouble ticket from the contractor's help desk. Conflicts, or requests outside of the scope of the contract will be referred to the COR.
Contractor Responsibility	The government will work with the government representatives to determine the method of delivery. If there are problems, the contractor will contact the CTR for resolution.
Customer Responsibility	The government representative will work with the contractor to determine delivery methods and designate a primary and alternative receipt representative.
Frequency	Monthly
Measurement Techniques	The CTR will spot check documentation deliverables and determine when they were delivered. The contract will specify when the documents are to be delivered. The CTR will compare the delivery time designated in the contract with the actual delivery time to determine compliance with the thresholds. Actual delivery times will be determined by interviews, or the timestamp on documentation that has been e-mailed.
Reports	1. Hosting contract
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	13.1 Documentation Accuracy
Performance Metric	This measurement ensures the accuracy of the documentation that is delivered. For example, configuration data must be accurate and up to date for

	disaster recovery, testing, and software development purposes. It is not enough to simply deliver documentation; the information contained in that documentation must be timely and accurate.
Threshold Levels	The thresholds apply to all required documentation. Inaccuracy is a subjective determination made by the CTR. The document must contain more than three non-significant errors, or one significant error. The CTR will determine the criticality of the error with respect to its affect on the application and the business processes the application supports. Non-significant error would be addition errors that do not significantly affect the computational outcome, missing serial numbers on hardware configuration documentation, or fail to update equipment moves within the host environment. Significant errors would include failure to update the backup schedule with new systems, failing to update the software configuration documentation with new upgrades, or failing to produce installation procedures for a system. The thresholds for accurate documentation is as follows: Essential – Premier: 95%
Formula	The number of documents audited with no errors divided by the number of total document deliverables.
Assumptions	The CTR will be able to determine whether a problem is significant or not. Discussions with the program manager and the contractor may help to categorize the severity of the document oversight/error.
Contractor Responsibility	The contractor will determine the root cause of any documentation errors, and attempt to automate as much reporting as possible.
Customer Responsibility	The CTR will inform the contractor of any errors discovered in the documentation.
Frequency	Monthly
Measurement Techniques	The CTR will perform spot checks on the documentation. Most errors in the documentation will be discovered through problem resolution, red team vulnerability assessments, and configuration audits.
Reports	1. All required documentation is subject to audit. 2. Red team vulnerability assessments
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	13.2 License Management

Performance Metric	It is illegal to operate third party software without proper licenses. The contractor is responsible for ensuring that all software that is a part of the host environment is supported by valid licenses. License management also includes the application and it's associated databases.
Threshold Levels	All software must have current licenses. Shareware and freeware can be utilized in accordance with the acceptance agreements related to the specific software. The threshold for proper licenses are as follows: Essential – Premier: 95%
Formula	None
Assumptions	Government Off the Shelf (GOTS) software will not have to have a license.
Contractor Responsibility	The contractor must have a process in place to ensure that all software in the host environment, including the application, has valid licenses. If the license is based on the number of concurrent users, the contractor will be responsible for ensuring the users do not exceed the license agreement. The contractor will notify the government of licenses about to expire, as well as when licenses need to be renegotiated to support an expanding user base.
Customer Responsibility	Copies of all license agreements must be turned over to the contractor before the software can be utilized.
Frequency	Quarterly
Measurement Techniques	The CTR will conduct spot checks of the licenses against the software configuration documentation.
Reports	1. Software configuration documentation 2. Software licenses
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	13.3 Meeting Attendance
Performance Metric	The contractor must have a representative at all scheduled meetings. The contractor would not have been invited to the meeting if the business did not involve the contractor. Participation is necessary to ensure that time is not wasted waiting for contractor input, or decisions from the contractor. All contractor representatives are expected to be able to represent the contractor and make decisions. The contractor and the government must develop a schedule for the meetings that the contractor is expected to attend. Meetings other than those agreed upon in the schedule of meetings will not apply to this SLA.
Threshold Levels	Thresholds for attending scheduled meetings is as follows:

	Essential – Premier: 95%
Formula	The number of meetings with a contractor representative in attendance divided by the total number of scheduled meetings.
Assumptions	The contractor will make every effort to attend meetings that were not in the official schedule. If enough warning is given, meetings will be rescheduled. Rescheduling of meeting should be coordinated with the program manager's staff.
Contractor Responsibility	Ensure the individual attending the meeting has the ability to represent the interests of the contractor as a voting member.
Customer Responsibility	The customer must determine which meetings the contractor needs to attend. Once the meetings have been identified, then the government must work with the contractor to develop a schedule that both parties can agree to. The government will notify the CTR if the contractor has failed to attend any scheduled or rescheduled meetings. A copy of the notification will be sent to the contractor. It is not necessary to notify the CTR of rescheduled meetings.
Frequency	Monthly
Measurement Techniques	The government will notify the CTR and the contractor when the contractor has failed to attend a scheduled meeting. If there are any challenges from the contractor, the CTR will compare the schedule of meetings against the minutes for those meetings. The meeting minutes will contain the attendees. If no contractor representatives were in attendance, then the challenge will not be accepted. If in the opinion of the CTR and program manager, the contractor has provided enough warning to reschedule a meeting, that particular meeting will not be counted in the SLA computations.
Reports	1. Meeting schedule 2. Meeting minutes 3. Notification from the government of missed meetings
Person Responsible for Verification	The CTR is responsible for verification.

Performance Category	13.4 Change Management Processes
Performance Metric	Before a software or hardware change (modification, upgrade, new version, updated hardware, etc…) is implemented, it must first be approved by the change

	review board. Maintaining control of software and hardware configuration changes is essential to the ensuring architectural conformity, disaster recovery, compatibility with other software, interoperability, and quality assurance. The metric will be the percentage of hardware and software changes that were executed in accordance with the change management procedures.
Threshold Levels	The thresholds for abiding by the change management procedures is as follows: Enhanced – Premier: 95%
Formula	The number of hardware and software changes that were executed in accordance with the change management processes divided by total number of changes executed.
Assumptions	All change review board meetings are documented to capture those changes that have been approved, and disapproved. All configuration changes will be documented.
Contractor Responsibility	Ensure change management procedures are followed. If changes are needed before the board can convene, the contractor will work with the government to gain approval.
Customer Responsibility	The government must hold change review boards often enough to support change requirements. If changes are occurring at a rate that is not supported by the change review boards, the government will appoint a representative to review and approve urgent changes.
Frequency	Monthly
Measurement Techniques	The CTR will review the configuration documentation and the system and monitoring logs to ensure that only approved changes were installed on the system.
Reports	1. System logs 2. Configuration documentation 3. Change Review Board Meetings 4. Monitoring logs
Person Responsible for Verification	The CTR is responsible for verification.
Escalation Procedures	The COR will resolve any disputes regarding contractual interpretations, or categorization of document errors.
Contractual Exceptions	None
Penalties/Rewards	Minor delivery penalty: No monetary penalty • Any threshold values were exceeded. Minor accuracy, attendance, and change management

	penalty: 5% monthly rate • Any threshold values were exceeded. 13.0 Major delivery penalty: 10 % monthly rate • More than 3 minor penalties within the year • Daily reports exceeding 3 days • Weekly reports exceeding 4 days • Monthly reports exceeding 7 days • Quarterly reports exceeding 7 days • Annual reports exceeding 10 days 13.1 Major accuracy penalty: 20 % monthly rate • More than 3 minor penalties within the year • More than 1 significant error in one month 13.2 Major license penalty: 25% monthly rate • Any threshold values were exceeded. 13.3 Major attendance penalty: 10% monthly rate • More than 3 minor penalties within the year • Less than 80% attendance in one month 13.4 Major change management penalty: 20% • More than 3 minor penalties within the year • Less than 80% adherence to the policy in one month Any malicious or intentional inaccuracies in required documentation directly affecting SLAs may result in termination of the contract.

Papers with presentations

None

Presentations alone

L. T. Gaines, and J. B. Michael, Affects of Service Level Agreements of IT Systems Management. Acquisition of Software-Intensive Systems Conference, Arlington VA., Jan. 2003 (Invited)

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
8725 John J. Kingman Rd., STE 0944
Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library, Code 013 2
Naval Postgraduate School
Monterey, CA 93943-5100

3. Research Office, Code 09 1
Naval Postgraduate School
Monterey, CA 93943-5138

4. J. Bret Michael, Code CS/Mj 1
Department of Computer Science
Naval Postgraduate School
Monterey, CA 93943-5118
bmichael@nps.navy.mil